ADTRAN Operating System (AOS)

AOS Version R14.4.0

Command Reference Guide

60000CRG0-35AV
September 2024

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, service marks, or trade names of their respective holders.

To the Holder of this Manual

The contents of this manual are current as of the date of publication. Adtran reserves the right to change the contents without prior notice.

In no event will Adtran be liable for any special, incidental, or consequential damages or for commercial losses even if Adtran has been advised thereof as a result of issue of this publication.

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. Adtran OFFERS NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF Adtran EQUIPMENT OR SOFTWARE. THEREFORE, Adtran IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS. Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

Software Licensing Agreement

Each Adtran product contains a single license for Adtran supplied software. Pursuant to the Licensing Agreement, you may: (a) use the software on the purchased Adtran device only and (b) keep a copy of the software for backup purposes. This Agreement covers all software installed on the system, as well as any software available on the Adtran website. In addition, certain Adtran systems may contain additional conditions for obtaining software upgrades.

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000
www.adtran.com
60000CRG0-35AV

Printed in the U.S.A.

Conventions

Notes provide additional useful information.

Cautions signify information that could prevent service interruption.

Warnings provide information that could prevent damage to the equipment or endangerment to human life.

Service and Warranty

For information on the service and warranty of AdtranAdtran products, visit the Adtran website at http://www.adtran.com/support.

Export Statement

An Export License is required if an Adtran product is sold to a Government Entity outside of the EU+8 (Austria, Australia, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the United Kingdom). This requirement is per DOC/BIS ruling G030477 issued 6/6/03. This product also requires that the Exporter of Record file a semi-annual report with the BXA detailing the information per EAR 740.17(5)(e)(2).

DOC - Department of Commerce
BIS - Bureau of Industry and Security
BXA - Bureau of Export Administration

Table of Contents

REFERENCE GUIDE INTRODUCTION

This manual provides information about connecting your product, using the Adtran Operating System's (AOS) command line interface (CLI), and executing the commands available with the NetVanta series units and certain Total Access series units.

If you are new to the AOS CLI, please take a few moments to review the information provided in the sections which follow.

If you are already familiar with Adtran NetVanta and Total Access units and looking for information on a specific command or group of commands, please proceed to *Command Descriptions on page 27* of this guide.

AOS UNIT INTRODUCTION

External Parts

To connect and use your new AOS unit, first familiarize yourself with the external features of the unit. For products that have a serial port, it can be located on either the back or front of the unit. If available, this port is marked **CONSOLE** and connects the unit directly to your PC via a standard DB-9 serial cable.

Other features vary from unit to unit, but include power connections, physical interface connections, and status LEDs along the front that indicate the status of your unit. For a more detailed description of your particular product, please refer to the appropriate hardware installation guide available online at https://supportcommunity.adtran.com.

Internal Parts

In order to fully understand product operation and receive the full benefit of the included guides, you should be familiar with the unit's internal parts, which can be divided into five main categories.

1. ROM - Read Only Memory

Read only memory (ROM) is a permanent form of memory stored in chips within the unit and houses information used by the AOS unit on initial startup. Examples of information stored in ROM are the Power-On Self Test, which initializes upon boot up and checks the unit's functionality; the Bootstrap Startup Program, which actually starts the unit; and the basic form of the AOS software.

2. Flash Memory

Flash memory is memory located in a memory chip that is not only erasable, but also reprogrammable, allowing for software upgrades without chip removal. The flash memory in your unit contains the full AOS and can be used to house copies of the configuration files and application images that are used at initial unit startup.

3. CompactFlash® Memory

CompactFlash memory (where available) is memory located on a CompactFlash memory card that is erasable and reprogrammable, allowing software upgrades without chip removal. The CompactFlash memory in your unit can be used to house copies of the configuration files and application images that are used at initial unit startup.

4. RAM - Random Access Memory

Random Access Memory (RAM) is the computer memory that functions as the working memory of your AOS unit. When the unit is on, the RAM provides memory for caching, packet buffering, holding routing tables, and housing the running operating system. When the unit is first powered on, RAM executes the application codes from flash memory and the startup configurations from nonvolatile random access memory (NVRAM), and when the unit is powered off or reset, RAM loses all data.

5. NVRAM - Nonvolatile Random Access Memory

NVRAM is the general name for any RAM that does not lose its information at power down (for example, flash memory). In this case, NVRAM has a separate memory function than the flash memory and is used to house the unit's startup configurations.

6. Interfaces

Interface is the term used to describe how your unit connects with its outside environment. There are a variety of interface categories, as well as interface types. Interface categories include line interfaces, physical interfaces, virtual, and wireless interfaces.

- Line interfaces describe the way you are communicating with your unit (for example, by console or Telnet).
- Physical interfaces describe the way your unit is physically connected to other units or devices (for example, via Ethernet, T3, serial, or asymmetric digital subscriber line (ADSL)).
- Virtual interfaces describe the way your unit receives information, whether by Frame Relay, Point-to-Point Protocol (PPP), virtual local area network (VLAN), or asynchronous transfer mode (ATM), to name a few.
- Wireless interfaces describe the way your unit receives or transmits information without a physical connection. The connectivity is provided through a radio transmission. There are multiple components to a wireless local area network (WLAN) which include access points (APs), radio interfaces, and virtual access points (VAPs).

The user can configure a unit's interfaces through the interface command sets (refer to *Configuration Command Sets on page 16*).

INTRODUCTION TO COMMAND LINE INTERFACE

The CLI is a method used to communicate with your AOS unit. While it describes the method used to communicate, such as by console or Telnet, it also refers to the way information is passed to the unit. As a text-based user interface, the CLI prompts you to input commands line by line when you interface with the AOS unit (hence the name command line interface).

Introduction to Commands

The most important part is understanding that your commands make the AOS unit function. The right commands lead to a fully functioning unit, whereas improperly entered or forgotten commands prevent the unit from functioning. To properly use commands, you must understand what function you want the AOS unit to complete and what syntax the unit understands as instructions. Each command has its own role within the operating system, and it is the responsibility of the operator to become familiar with specific commands and command sets.

How Commands Function

Commands are composed of two main parts. The most important part is the command itself, or the command word. Most command words are short and straightforward (for example, **do**, **exit**, or **configure**). Command words are entered immediately after the command prompt in the CLI.

The second part of a command is its argument. An argument is a specification that modifies the command. In the command **show flash**, **show** is the command word and **flash** is the argument because it modifies the command **show**. Commands can have any number of arguments, depending upon the action required of the unit, and in some instances you have a choice of arguments to use.

Optionally, some commands use variables with the argument to specify information relevant only to your AOS unit. These variables are identified with the greater-than (<) and less-than symbols (>). The description of the information required is contained within the symbols and displayed in *italics*. For example, the following command provides the command **clock**, argument **set**, and includes the variables <*time*>, <*day*>, <*month*>, and <*year*>:

clock set <*time*> <*day*> <*month*> <*year*>

AOS Command System

Adtran products, training tools, and manuals follow a specific system for entering and referencing commands. Items that are typed in **bold** are the required commands and arguments for a certain action. In the following documentation, you will see commands in bold after an example prompt. They look similar to this:

>enable
#configure terminal
(config)**#line telnet 4**
(config-telnet4)#

In the example above, the characters >, #, (config)#, and (config-telnet4)# are the prompts after which commands are entered. In this example, the words in bold (**enable**, **configure terminal**, and **line telnet 4**) are the entire commands and constitute what should be typed after the prompt. It is important to pay attention to the prompt you are given when communicating with your unit, because certain commands only work in certain modes, which are signified by the prompt. The different prompts and modes are discussed later in this guide.

In certain commands, you are given a choice of arguments. If this is the case, the manual or guide will place the argument in brackets separated by a vertical bar (|) between your choices as seen in this example:

#show [flash | cflash]

Again, remember the # is your prompt, the command word is **show**, and your choices of arguments are **flash** and **cflash**.

Certain commands require you to enter your own information which are called variables. Information within a command line that pertains to your personal unit is set off with the greater-than (<) and less-than symbols (>). The description of the information required is contained within the greater-than and less-than symbols and is displayed in *italics*. For example:

#copy <*file source location*> <*config-file*> **tftp**

In this case, # is your prompt, the command word is **copy**, the information needed from you is the source location of the file you want to copy (<*file source location*>) and the configuration file type (<*config-file*>), and **tftp** indicates the location to which to copy the file.

USING THE CLI

This portion of the Command Reference Guide introduces you to the basic concepts and strategies associated with using the AOS CLI.

Connecting the Unit

For the initial use, the unit should be connected to a PC with VT100 terminal emulation program. To connect the unit, simply connect a DB-9 straight-through male-to-female serial cable to the **CONSOLE** port and to your PC.

Accessing the CLI from Your PC

All products using the AOS are initially accessed using a PC with VT100 terminal emulation program (such as HyperTerminal or PuTTY) and console port cable. If you don't have a VT100 terminal emulation program, you can download PuTTY from the Internet.

Emulation Settings

Once you have connected to the unit, adjust the program settings as follows:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control

If you are using a VT100 terminal emulation program, name your new connection and set up the new connection. Verify **COM 1** is the type of connection you are using. Once you have entered the program settings and applied them, you should be presented with a terminal window with which to interface with your unit.

Unit Boot Up

After configuring your PC, provide power to the AOS unit and turn it on. The AOS unit begins the boot up process, which includes the following:

- The Power-On Self Test runs. This test checks the unit hardware for normal operation. The hardware includes the central processing unit (CPU), the memory, and the interfaces.
- The Bootstrap Startup Program (factory set in the ROM) runs.
- The Bootstrap Startup Program is read by the unit to discover the proper source for the operating system image.
- The operating system image is loaded into RAM.
- The configuration file saved in NVRAM is loaded into RAM, where it is accessed by the unit and then executed one line at a time.

If no configuration file is found in NVRAM (there will not be one found on initial setup), you are presented with the following prompt on your PC's VT100 terminal emulation screen:

```
Session Now Available
Press RETURN to get started
```

After pressing return, a prompt appears for communication with your unit.

Understanding Command Modes

As you begin communication, you should understand the command modes. Just as there are different levels of commands in the CLI, there are different modes for commands within AOS itself. Each command mode enables the user to access more commands, and make more changes in the unit's configuration.

The CLI has four command modes: Basic, Enable, Application, and Global. The four command modes are organized in a four-tiered hierarchy with Basic at the bottom, then Enable, then Application, and Global at the top.

Basic Mode

Interaction with your unit begins at the Basic mode. The commands supported at this command tier are limited, as is interaction with the unit itself. The Basic mode prevents users without access to the higher tiered commands from changing the preferred configurations of the unit. The following table describes the Basic mode.

Mode	Access By...	Mode Prompt	Accessible Commands
Basic	Beginning an AOS session	>	• Display system information • Perform traceroute and ping functions • Open a Telnet session

For more information on the Basic mode, please refer to *Basic Mode Command Set on page 45*.

Enable Mode

Enable mode is one step up from the Basic mode. Adtran suggests that a password be required to access the Enable mode. Refer to the quick start guides shipped with your unit and located online at https://supportcommunity.adtran.com for more information on configuring a password.

From the Enable mode, you can access the configurations of your product, as well as handle how your unit boots and runs, among other things. The following table describes the Enable mode.

Mode	Access By....	Mode Prompt	Accessible Commands
Enable	Entering **enable** while in the Basic mode as follows: **>enable**	#	• Manage the startup and running configurations • Enable and disable **debug** commands • View **show** command output • Enter any of the configuration modes

For more information regarding the Enable command set, refer to the *Enable Mode Command Set on page 94*.

Global Mode

The Global mode is the highest level tier within AOS. The Global mode allows the user to make changes regarding the entire product system. All of your system's configurations are accessed through the Global mode. From this level, you can access not only line configurations, router configurations, and interface configurations, but also any other configurations or parameters on your system. The following table describes the Global mode.

Mode	Access By...	Mode Prompt	Accessible Commands
Global	Entering **config** while at the Enable mode as follows: **>enable** **#** **#config**	(config)#	• Set the system's Enable-level password(s) • Configure the system global IP parameters • Configure the SNMP parameters • Enter any of the configuration modes

For more information on the Global mode, refer to *Global Configuration Mode Command Set on page 1149*.

Application Mode

The Application mode is accessed from the Enable mode. Enable mode access is necessary to access the Application mode. This mode is used to configure applications on the AOS unit, such as Y.1731 or network synchronization (Network Sync). The following table describes the Application mode.

Mode	Access By....	Mode Prompt	Accessible Commands
Application	Entering **application** while in the Enable mode as follows: **>enable** **#application**	(app)#	• Configure the Y.1731 application • Configure the Network Sync application

For more information on the Application mode, refer to *Application Command Sets on page 1991*.

Understanding Configurations

Configurations are the means by which you set up your unit and system according to your personal requirements and preferences. You must configure your unit to work within your network, based on your hardware and communication systems.

All configurations are accessed through the Global Configuration mode. By typing in **config** at the Enable mode prompt, you will be ready to specify the configuration you want to access.

For each configuration, enter the word or phrase that correlates with the system you are configuring. There are different command sets for each type of configuration. These command sets are detailed in the following section.

Configuration Command Sets

The configuration command sets are broken down into categories of similar functions. For example, all commands pertaining to configuring the interfaces are grouped together, as are commands for configuring routing, configuring security and services, and so on. The following sections introduce each category of command sets and the command subsets organized within them in this guide. For a complete list of command sets and their reference pages, refer to *Command Descriptions on page 27*.

Interface Command Sets

Interface commands configure the physical and virtual interfaces in which you communicate with your device. Not all AOS units have all of the interface types explained in this section. Wireless interfaces are also included for the units that support it. The following table gives an example of the each interface command set. For a more detailed description, refer to *Command Descriptions on page 27*.

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
Line Interface	Specifying a line (console, Telnet, SSH) at the Global Configuration mode prompt as follows: >**enable** **#config terminal** (config)**#line console 0**	(config-con0)#	• Gain initial access to the unit before configuring network settings • Configure the console or terminal settings (data rate, login password, etc.) • Create Telnet logins and specify their parameters (login password, etc.)
Physical Interface	Specifying an interface at the Global Configuration mode prompt as follows: >**enable** **#config terminal** (config)**#interface adsl 0/1**	(config-adsl0/1)#	• Configure the parameters of your physical connections • Configure your physical network
Virtual Interface	Specifying an interface at the Global Configuration mode prompt as follows: >**enable** **#config terminal** (config)**#interface frame-relay 1**	(config-fr 1)#	• Determine the parameters of information flow • Configure your unit's methods for communicating with other devices • Configure network protocols; such as ATM, Frame Relay, PPP, VLAN, etc.
Wireless Interface	Specifying a wireless interface at the Global Configuration mode prompt as follows: >**enable** **#config terminal** (config)**#interface dot11ap 1 ap-type nv16x**	(config-dot11ap 1)#	• Configure your unit's wireless parameters; wireless access points (APs), access point radios, and virtual access points (VAPs) • Configure how your wireless network will integrate with your wired network

Carrier Ethernet Command Sets

Carrier Ethernet interfaces consist of virtual interfaces that are only available on specific AOS products used to interface with Metro Ethernet network (MEN) and carrier Ethernet technologies. In this guide, commands pertaining to these virtual interfaces are listed in their own section to separate them from the more commonly used interfaces. The Carrier Ethernet section is divided into EFM NIM 2 Ethernet, Carrier Ethernet Services, and Y.1731. Each section has been further divided into additional sections containing command sets for specific configuration functions dealing with each of these technologies.

Ethernet in the First Mile (EFM) NIM2 Ethernet command sets pertain to the Metropolitan Ethernet Forum (MEF) Ethernet interface which functions as the user-network interface (UNI) in AOS products with the second-generation EFM network interface modules (NIMs). The MEF Ethernet interface is a virtual interface used by AOS products to interface with the MEN and carrier Ethernet technologies. The MEF Ethernet interface is used as the Layer 2 and 3 wide-area network (WAN) interface.

Carrier Ethernet Services command sets pertain to the MEF Ethernet virtual connection (EVC) which connects two endpoints (for example, the EFM group and the MEF Ethernet interface) and passes Ethernet service frames through these endpoints.

Y.1731 command sets pertain to EFM configurations on the AOS device that use the Y.1731 protocol. The Y.1731 commands allow you to configure how your unit will behave as it employs Y.1731 EFM over your network.

The following table gives an example of the carrier Ethernet commands. For a more detailed listing of commands, refer to *Command Descriptions on page 27*.

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
EFM NIM2 Ethernet	Specifying a MEF interface at the Global Configuration mode prompt as follows: >**enable** **#configure terminal** (config)**#interface mef-ethernet 0/1**	(config-mef-ethernet 0/1)#	• Configure the MEF Ethernet interface • Configure EFM bonding groups to provide EFM capabilities across WAN interfaces • Configure EVC attributes • Set parameters for policer policies to limit outbound traffic bandwidth • Configure EVC map attributes and associate with an EVC and a UNI

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
Carrier Ethernet Services	Specifying an EVC from the Global Configuration mode prompt as follows: >enable **#configure terminal** (config)**#evc DATA** (config-evc-DATA)#	(config-evc-DATA) #	• Create and configure EVCs • Configure EFM groups. • Configure EVC queues, policer policy, map and shaper. • Configure the system control EVC • Set parameters for inband IP network interface for system management and control
Y.1731	Specifying which Y.1731 feature you wish to configure at the Global Configuration mode prompt as follows: **>enable** **#configure terminal** (config)**#ethernet y1731 meg char-string MEG1** (config-y1731-meg MEG1)#	(config-y1731-meg MEG1)#	• Specify the MEF traffic shaper rate • Specify the interface to which the MEF shaper is applied • Configure the Y.1731 maintenance entity group (MEG) and Y.1731 local MEG endpoint (MEP) • Specify the frame delay, frame loss, and traffic shaper settings for Y.1731 traffic • Use Show commands related to Y.1731 settings

Routing Protocol Command Sets

The routing command sets serve two functions. Routing commands not only address the manner in which your unit routes and disseminates information, but they also provide an additional level of security for your network. Routing commands include parameters, such as AS path list, community list, and network monitoring, and they determine whether your unit routes via Routing Information Protocol (RIP), open shortest path first (OSPF), or protocol-independent multicast (PIM) sparse.

The following table gives an example of the routing command sets. For a complete list of routing commands, refer to the *Command Descriptions on page 27*.

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
Routing	Specifying which routing parameter you wish to set at the Global Configuration mode prompt as follows: **>enable** **#config** (config)**#router ospf**	(config-ospf)#	• Determine which devices are compatible with your network • Determine how your unit routes traffic and information • Configure network monitoring probes, tracks, and responders • Configure the unit's route map

Security and Services Command Sets

The security and services command sets provide methods for you to configure additional security for your unit, as well as determine the types of services you want your unit to perform. Included in these command sets are quality of service (QoS) maps, Dynamic Host Configuration Protocol (DHCP) pools, and route map configurations.

The following table includes an example of the security and services commands. For a more detailed listing of the command sets, refer to *Command Descriptions on page 27*.

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
Security and Services	Specifying the service you would like to perform at the Global Configuration mode prompt as follows: **>enable** **#config** (config)**#aaa group server radius myServer**	(config-sg-radius)#	• Map the quality of a variety of services • Set the parameters for the DHCP • Configure access control lists (ACL) and access control policies (ACP) for network security • Configure security services for Radius and Tacacs+ Groups.

Voice Command Sets

Voice command sets configure all aspects of voice functionality within your network. These commands only pertain to AOS devices that support voice as part of their feature set.

The following table describes the different voice command subsets and explains briefly each command set. For a more detailed description, refer to *Command Descriptions on page 27*.

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
Voice Accounts	Specifying the voice account you would like to configure at the Global Configuration mode prompt as follows: **>enable** **#config** (config)**#voice user 4444**	(config-4444)#	• Set parameters for user accounts, line accounts, and loopback accounts • Specify the behaviors and permissions of these accounts within the voice network
Voice Groups	Specifying the voice group you would like to configure at the Global Configuration mode prompt as follows: **>enable** **#config** (config)**#voice ring-group 1234**	(config-1234)#	• Set parameters for ring groups, operator groups, trunk groups, paging groups, and more • Specify the behaviors and permissions of voice groups, as well as define the members of the groups

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
Voice Services	Specifying the voice service you would like to configure at the Global Configuration mode prompt as follows: **>enable** **#config** (config)**#voice autoattendant Example 1212**	(config-aa1212)#	• Set parameters for class of service (CoS) on the voice network • Configure voice features (voicemail, auto attendant, Music on Hold, Find Me Follow Me, etc) • Use voice quality monitoring reporters • Specify the behaviors and permissions of voice features within the network
Voice Trunks	Specifying the voice trunk type you would like to configure at the Global Configuration mode prompt as follows: **>enable** **#config** (config)**#voice trunk t01**	(config-t01)#	• Set parameters for analog trunks, T1 trunks, Session Initiation Protocol (SIP) trunks, and more • Specify the behaviors and permissions of these trunks

Virtual Private Network Parameter Command Sets

The virtual private network (VPN) parameter command sets deal with the encryption and security on your private network. To allow you the utmost in security, the VPN parameter commands allow you to configure how your unit will behave as it communicates with other devices. VPN command sets allow you to configure Internet key exchange (IKE) parameters, crypto parameters, and certificate parameters.

The following table gives an example of the VPN parameter commands. For a more detailed listing of commands, refer to *Command Descriptions on page 27*.

Command Set	Accessed By...	Sample Prompt	With This Set You Can...
VPN Parameters	Specifying which parameter you wish to set at the Global Configuration mode prompt as follows: **>enable** **#config** (config)**#crypto ca certificate chain MyProfile**	(config-cert-chain)#	• Determine how your unit authenticates communication • Set the parameters for keeping your unit secure

Using CLI Shortcuts

The AOS CLI provides several shortcuts to help you configure your AOS product more easily. See the following table for descriptions.

Shortcut	Description
Up arrow key	To redisplay a previously entered command, use the up arrow key. Continuing to press the up arrow key cycles through all commands entered, starting with the most recent command.
<Tab> key	Pressing the **<Tab>** key after entering a partial (but unique) command will complete the command, display it on the command prompt line, and wait for further input.
?	The AOS CLI contains help to guide you through the configuration process. Using the question mark, do any of the following: Display a list of all subcommands in the current mode. For example: (config-t1 1/1)**#coding ?** ami - Alternate Mark Inversion b8zs - Bipolar Eight Zero Substitution Display a list of available commands beginning with certain letter(s). For example: (config)**#ip d?** default-gateway dhcp-server domain-lookup domain-name domain-proxy Obtain syntax help for a specific command by entering the command, a space, and then a question mark (?). The AOS CLI displays the range of values and a brief description of the next parameter expected for that particular command. For example: (config-eth 0/1)**#mtu ?** <64-1500> - MTU (bytes)
<Ctrl + A>	Jump to the beginning of the displayed command line. This shortcut is helpful when using the **no** form of commands (when available). For example, pressing **<Ctrl + A>** at the following prompt will place the cursor directly after the **#**: (config-eth 0/1)**#ip address 192.33.55.6**
<Ctrl + E>	Jump to the end of the displayed command line. For example, pressing **<Ctrl + E>** at the following prompt will place the cursor directly after the **6**: (config-eth 0/1)**#ip address 192.33.55.6**
<Ctrl + U>	Clears the current displayed command line. The following provides an example of the **<Ctrl + U>** feature: (config-eth 0/1)**#ip address 192.33.55.6** (Press **<Ctrl + U>** here) (config-eth 0/1)#
auto finish	You need only enter enough letters to identify a command as unique. For example, entering **int t1 1/1** at the Global Configuration mode prompt provides you access to the configuration parameters for the specified T1 interface. Entering **interface t1 1/1** would work as well, but is not necessary.

Searching for Commands in the CLI

The AOS CLI contains several thousand commands, accessible through various command modes and command sets. Finding a specific command, particularly if you do not know the command set in which the command is located, or the entire syntax of the command, can be difficult. To make it easier to find specific commands in the CLI, an algorithmic search tool is provided. This search tool scans the entire CLI for the command you specify, scanning all command modes and sets, and displays the commands that match the specified criteria. This feature can be more useful than the **?** CLI shortcut because it gives the entire syntax of the matching commands, and the search is not limited to the currently active command set.

To search for a command in the CLI, enter the **find** <*input*> command at the Enable mode prompt. The <*input*> parameter is a text string of the command for which you are searching, for example, **sip proxy**. The following example tells the CLI to search for all commands that match **sip pr**. The output displays the matching commands and their associated command set(s).

```
>enable
#find sip pr
Searching....Found 4 commands
Root                : clear sip proxy
Root                : debug sip proxy
Root (2)            : show sip proxy
configterminal (3)  : sip proxy
```

The above example displays all commands in the CLI that match **sip pr**, combining any results that are similar. Note the (2) in the Root command set, indicating two commands with similar syntax in the Enable mode match the criteria, and the (3) in the configterminal command set, indicating three commands with similar syntax in the Global Configuration mode match the search criteria. Command search results are considered to be similar based on three criteria: they are in the same command set (Root or configterminal in the previous example), they use the same root command (show sip proxy or sip proxy in the previous example), and they meet the search criteria (both match sip proxy in the previous example). Search results are combined by default, but you can optionally choose to display all commands by entering the **find /no suppress** <*input*> command for your search. For example, to list all commands that match **sip pr**, enter the command as follows (note the difference in the command output from the previous example):

```
>enable
#find /no suppress sip pr
Searching...Found 7 commands
Root                : clear sip proxy
Root                : debug sip proxy
Root                : show running-config sip proxy
Root                : show sip proxy
configterminal      : sip prefer
configterminal      : sip privacy
configterminal      : sip proxy
```


In addition to specifying that search results are not combined, you can also limit search results to the active command set by entering the **find /current-set** <*input*> command. The optional **current set** parameter limits the search to the current active command set. For example, if you were searching for packet capture commands, and searched all of the CLI, the search returns 13 available matching commands. If you limit the search to the Enable mode only, using the **/current-set** parameter, the search returns only the two packet capture commands available in the Enable mode (note that similar commands are combined in the search results by default; entering the optional **/no-suppress** parameter in addition to **/current-set** parameter will display all matching commands in the set).

```
>enable
#find /current-set packet-capture
Searching... Found 2 commands
debug packet-capture
show packet-capture: (2)
```

Wildcards can also be used when searching for commands in the CLI. Wildcards can be beneficial when you do not know the entire syntax of the command you are looking for. Use the ***** character to specify the search matches anything in place of the *****. Enter the command as follows to search using wildcards:

```
>enable
#find sip*tcp
Searching... Found 3 commands
voice-trunk-sip (2)    : sip-server primary * tcp
configterminal (4)     : sip tcp
configterminal : voip name-service host * sip tcp
```

Performing Common CLI Functions

The following table contains descriptions of common CLI commands.

Command	Description
exit	The **exit** command exits the current command set and returns to the previous command set. For example, when entering **exit** in the Global Configuration mode, you will be returned to the Enable mode. >**enable** **#configure terminal** (config)**#exit** > Your location in the CLI hierarchy determines the command set you will return to when entering this command. If you enter **exit** in the Enable mode you will exit the CLI completely.

Command	Description
end	The **end** command exits the current command set and returns to the Enable mode, no matter what your current location is in the CLI hierarchy. For example, when entering **end** in the T1 Interface Configuration mode, you are returned to the Enable mode prompt. >**enable** **#configure terminal** (config)**#interface t1 1/1** (config-t1 1/1)**#end** >
do	The **do** command provides a way to execute commands in other command sets without having to exit the current command set. The following example shows the **do** command used to view the Frame Relay interface configuration while in the T1 interface command set: (config)**#interface t1 1/1** (config-t1 1/1)**#do show interfaces fr 7**
no shutdown	To activate an interface, enter **no shutdown** from the interface configuration mode. For example, the following command activates the T1 1/1 interface: (config)**#interface t1 1/1** (config-t1 1/1)**#no shutdown t1 1/1**
no	To disable a feature or return a command to its default setting, enter **no** before the command. The following example disables the voice debug messages. >**no debug voice**
copy running-config startup-config	Entering this command in the Enable mode saves changes made to the configuration. This command copies your changes to the unit's NVRAM. Once the save is complete, the changes are retained even if the unit is shut down or suffers a power outage.
show running config	Entering this command in the Enable mode displays the current configuration.
debug	Use the **debug** commands in the Enable mode to troubleshoot problems you may be experiencing on your network. These commands provide additional information to help you better interpret possible problems. For information on specific debug commands, refer to the debug section beginning on *page 285*.
undebug all	Entering this command in the Enable mode turns off any active debug commands.

*The overhead associated with the **debug** command takes up a large portion of your AOS product's resources, and at times can halt other processes. It is best to use the **debug** command only during times when the network resources are in low demand (nonpeak hours, weekends, etc.).*

Understanding CLI Error Messages

The following table lists and defines some of the more common error messages given in the CLI.

Message	Helpful Hints
%Ambiguous command %Unrecognized command	The command may not be valid in the current command mode, or you may not have entered enough correct characters for the command to be recognized. Try using the **?** command to determine your error. Refer to *Using CLI Shortcuts on page 21* for more information.
%Invalid or incomplete command	The command may not be valid in the current command mode, or you may not have entered all of the pertinent information required to make the command valid. Try using the **?** command to determine your error. Refer to *Using CLI Shortcuts on page 21* for more information.
%Invalid input detected at "^" marker	The error in command entry is located where the caret (^) mark appears. Enter a question mark at the prompt. The system displays a list of applicable commands or gives syntax information for the entry.

COMMAND DESCRIPTIONS

This portion of the guide provides a detailed listing of all available commands for the AOS CLI (organized by command set). Each command listing contains pertinent information, including the default value, a description of all subcommand parameters, functional notes for using the command, and a brief technology review. To search for information on a group of commands within a particular command set, use the linked references given below:

System Command Sets

Application Command Sets

Interface Command Sets

Line Interface

Physical Interface

Carrier Ethernet Command Sets

Y.1731

Routing Protocol Command Sets

BGP

Network Monitoring

OSPFv2 and OSPFv3

Routing

Security and Services Command Sets

Access Control Lists and Policies

DHCP

Services

Voice Command Sets

Voice Accounts

Voice Groups

Voice Services

Voice Trunks

VPN Parameter Command Sets

Certificate

Crypto Map

IKE

COMMAND SET ACCESS PATH QUICK REFERENCE GUIDE

Application Command Sets

Command Set	Sample Access Path	For Full Command List, See...
Network Sync Application	>**enable** **#application** (app)#	*page 1992*
Y.1731 Application	>**enable** **#application** (app)**#ethernet y1731 meg char-string MEG1 3 100** (app-y1731 100)#	*page 1997*

Interface Command Sets

Line Interface Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Console	(config)**#line console 0** (config-con 0)#	*page 2021*
SSH	(config)**#line ssh 0 4** (config-ssh0-4)#	*page 2038*
Telnet	(config)**#line telnet 0 4** (config-telnet0-4)#	*page 2054*

Physical Interface Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
ADSL	(config)**#interface adsl 0/1** (config-adsl 0/1)#	*page 2072*
BRI	(config)**#interface bri 1/2** (config-bri 1/2)#	*page 2079*
Cellular	(config)**#interface cellular 1/1** (config-cellular 1/1)#	*page 2105*
DDS	(config)**#interface dds 1/1** (config-dds 1/1)#	*page 2121*
DSX-1	(config)**#interface t1 1/2** (config-t1 1/2)#	*page 2129*
E1	(config)**#interface e1 1/1** (config-e1 1/1)#	*page 2139*
Ethernet	(config)**#interface ethernet 0/1** (config-eth 0/1)#	*page 2156*

Command Set	Sample Access Path	For Full Command List, See...
Ethernet Subinterface	(config)#**interface ethernet 0/1.1** (config-eth 0/1.1)#	*page 2156*
Ethernet Subinterface for Layer 3 Services	(config)#**interface ethernet 0/1.1** (config-eth 0/1.1)#	*page 2156*
Gigabit Ethernet	(config)#**interface gigabit-ethernet 0/3** (config-giga-eth 0/3)#	*page 2156*
Gigabit Switchport	(config)#**interface gigabit-switchport 0/3** (config-giga-swx 0/3)#	*page 2156*
Switchport	(config)#**interface switchport 0/1** (config-swx 0/1)#	*page 2156*
Range of Ethernet Interfaces (in this example, **eth 0/1** through **eth 0/8**)	(config)#**interface range ethernet 0/1, 0/8** (config-eth 0/1, 0/8)#	*page 2156*
10 Gigabit Switchport	(config)#**interface xgigabit-switchport 0/3** (config-xgiga-swx 0/3)#	*page 2156*
FDL	(config)#**interface fdl 1/1** (config-fdl 1/1)#	*page 2357*
FXO	(config)#**interface fxo 0/1** (config-fxo 0/1)#	*page 2364*
FXS	(config)#**interface fxs 2/1** (config-fxs 2/1)#	*page 2375*
G.703	(config)#**interface e1 1/2** (config-e1 1/2)#	*page 2394*
HSSI	(config)#**interface hssi 1/1** (config-hssi 1/1)#	*page 2401*
Modem	(config)#**interface modem 1/2** (config-modem 1/2)#	*page 2405*
PRI	(config)#**interface pri 2** (config-pri 2)#	*page 2411*
Serial	(config)#**interface serial 1/1** (config-ser 1/1)#	*page 2432*
SHDSL	(config)#**interface shdsl 1/1** (config-shdsl 1/1)#	*page 2441*
T1	(config)#**interface t1 1/1** (config-t1 1/1)#	*page 2463*
T3	(config)#**interface t3 1/1** (config-t3 1/1)#	*page 2481*
T4	(config)#**interface t4 0/1** (config-t4 0/1)#	*page 2491*
VDSL	((config)#**interface vdsl 1/1** (config-vdsl 1/1)#	*page 2495*

Virtual Interface Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
ATM	(config)#**interface atm 1** (config-atm 1)#	*page 2498*
ATM Subinterface	(config)#**interface atm 1.1** (config-atm 1.1)#	*page 2502*
BVI	(config)#**bridge irb** (config)#**interface bvi 1** (config-bvi 1)#	*page 2593*
Demand	(config)#**interface demand 1** (config-demand 1)#	*page 2636*
Frame Relay	(config)#**interface frame-relay 1** (config-fr 1)#	*page 2727*
Frame Relay Subinterface	(config)#**interface frame-relay 1.16** (config-fr 1.16)#	*page 2748*
HDLC	(config)#**interface hdlc 1** (config-hdlc 1)#	*page 2888*
Loopback	(config)#**interface loopback 1** (config-loop 1)#	*page 2968*
Port Channel	(config)#**interface port-channel 1** (config-p-chan1)#	*page 3034*
PPP	(config)#**interface ppp 1** (config-ppp 1)#	*page 3060*
Tunnel	(config)#**interface tunnel 1 gre ip** (config-tunnel 1)#	*page 3211*
VLAN Configuration	(config)#**vlan 1** (config-vlan 1)#	*page 3356*
VLAN Database	(config)#**vlan database** (vlan)#	*page 3361*
VLAN Interface	(config)#**interface vlan 1** (config-interface-vlan 1)#	*page 3370*

Wireless Interface Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Access Point, NetVanta 150	(config)#**interface dot11ap 1 ap-type nv150** (config-dot11ap 1)#	*page 3494*
Access Point, NetVanta 160	(config)#**interface dot11ap 1 ap-type 16x** (config-dot11ap 1)#	*page 3550*

Command Set	Sample Access Path	For Full Command List, See...
Radio, NetVanta 150 or 160	(config)#**interface dot11ap 1/1** (config-dot11ap 1/1-bg)#	*page 3510* (for NetVanta 150), or *page 3567* (for NetVanta 160)
Virtual Access Point, NetVanta 150 or 160	(config)#**interface dot11ap 1/1.1** (config-dot11ap 1/1.1-bg)#	*page 3533* (for NetVanta 150), or *page 3585* (for NetVanta 160)

Carrier Ethernet Command Sets

EFM NIM2 Ethernet Interfaces Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
MEF EFM Group	(config)#**interface efm-group 1** (config-efm-group 1)#	*page 3599*
MEF Ethernet	(config)#**interface mef-ethernet 0/1** (config-mef-ethernet 0/1)#	*page 3604*
MEF Ethernet Subinterface	(config)#**interface mef-ethernet 0/1.1** (config-mef-ethernet 0/1.1)#	*page 3604*
MEF EVC	(config)#**mef evc DATA** (config-evc-DATA)#	*page 3674*
MEF EVC Map	(config)#**mef evc-map Map1** (config-evc-map-Map1)#	*page 3678*
MEF Policer Policy	(config)#**mef policer Policy1** (config-policer-Policy1)#	*page 3684*

Carrier Ethernet Services Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Carrier Ethernet EFM Group	(config)#**interface efm-group 1/1** (config-efm-group 1/1)#	*page 3691*
Carrier Ethernet EVC	(config)#**evc DATA** (config-evc-DATA)#	*page 3700*
Carrier Ethernet EVC Map	(config)#**evc-map Map1** (config-evc-map-Map1)#	*page 3705*
Carrier Ethernet Policer Policy	(config)#**policer Policy1** (config-policer-Policy1)#	*page 3719*
Carrier Ethernet Queue	(config)#**queue interface efm-group 1 3** (config-queue 3)#	*page 3728*
Carrier Ethernet Shaper	(config)#**shaper SHAPER1 0** (config-shaper shaper1 0)#	*page 3736*

Command Set	Sample Access Path	For Full Command List, See...
Carrier Ethernet Terminal Loopback	(config)**#ethernet loopback terminal TERMINAL 0** (config-eth-lbk-term TERMINAL 0)#	*page 3739*
Facility MAC Swap Loopback	(config)**#ethernet loopback facility FACILITY 0** (config-eth-lbk-fac FACILITY 0)#	*page 3742*
System Control EVC	(config)**#system-control-evc** (config-system-ctrl-evc)#	*page 3745*
System Management EVC	(config)**#system-management-evc** (config-system-mgmt-evc)#	*page 3843*

Y.1731 Interfaces Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
One-Way Frame Delay Monitoring Session	(config)**#ethernet y1731 meg char-string MEG1** (config-y1731-meg MEG1)**#local-mep 3** MEP 3 created (config-y1731-mep3)**#frame-delay one-way 500 priority 1** (config-y1731-frame-delay)#	*page 3923*
Two-Way Frame Delay Monitoring Session	(config)**#ethernet y1731 meg char-string MEG1** (config-y1731-meg MEG1)**#local-mep 3** MEP 3 created (config-y1731-mep3)**#frame-delay two-way 500 priority 1** (config-y1731-frame-delay)#	*page 3927*
Single-Ended Frame Loss Monitoring Session	(config)**#ethernet y1731 meg char-string MEG1** (config-y1731-meg MEG1)**#local-mep 3** MEP 3 created (config-y1731-mep3)**#frame-loss single-ended 500 priority 1** (config-y1731-frame-loss)#	*page 3935*
Single-Ended Synthetic Frame Loss Monitoring Session	(config)**#ethernet y1731 meg char-string MEG1** (config-y1731-meg MEG1)**#local-mep 3** MEP 3 created (config-y1731-mep3)**#frame-loss synthetic single-ended 500 priority 1** (config-y1731-frame-loss)#	*page 3942*
Y.1731 Local MEP	(config)**#ethernet y1731 meg char-string MEG1** (config-y1731-meg MEG1)**#local-mep 3** MEP 3 created (config-y1731-mep3)#	*page 3950*
Y.1731 MEG	(config)**#ethernet y1731 meg char-string MEG1** (config-y1731-meg MEG1)#	*page 3968*

Routing Protocol Command Sets

BGP Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
AS Path List	(config)#**ip as-path-list MyList** (config-as-path-list)#	*page 3978*
BGP	(config)#**router bgp 1** (config-bgp)#	*page 3981*
BGP Address Family	(config-bgp)#**address-family ipv4** (config-bgp-ipv4)#	*page 4001*
BGP Address Family Neighbor	(config-bgp-ipv4)#**neighbor 192.22.15.101** (config-bgp-ipv4-neighbor)#	*page 4022*
BGP Neighbor	(config-bgp)#**neighbor 192.22.15.101** (config-bgp-neighbor)#	*page 4041*
Community List	(config)#**ip community-list listname** (config-comm-list)#	*page 4058*

Network Monitoring Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Network Monitor Probe	(config)#**probe probe1 icmp-echo** (config-probe-probe1)#	*page 4062*
Network Monitor Probe Responder	(config)#**probe responder twamp** (config-responder-twamp)#	*page 4089*
Network Monitor Track	(config)#**track track1** (config-track-track1)#	*page 4098*

OSPFv2 and OSPFv3 Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
OSPFv2	(config)#**router ospf** (config-ospf)#	*page 4120*
OSPFv3	(config)#**router ospfv3 5** (config-ospfv3)#	*page 4141*
OSPFv3 IPv6 AF	(config)#**router ospfv3 5** (config-ospfv3)#**address-family ipv6 unicast** (config-ospfv3-ipv6)#	*page 4141*

Routing Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Route Map	(config)#**route-map MyMap permit 100** (config-route-map)#	*page 4168*
PIM Sparse	(config)#**router pim-sparse** (config-pim-sparse)#	*page 4201*
RIP	(config)#**router rip** (config-rip)#	*page 4205*
VRRPv3	(config)#**interface eth 0/1** (config-eth 0/1)#**vrrpv3 15 address-family ipv6** (config-if-vrrpv3 15)#	*page 4221*

Security and Services Command Sets

Access Control Lists and Policies Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Hardware ACL and Access Map	(config)#**ip hw-access-list extended Trusted** (config-ext-ip-hw-nacl)#	*page 4235*
IPv4 Access Control List	(config)#**ip access-list standard MATCHALL** (config-std-nacl)#	*page 4252*
IPv4 Access Control Policy	(config)#**ip policy-class PRIVATE** (config-policy-class)#	*page 4278*
IPv6 Access Control List	(config)#**ipv6 access-list standard MATCHALLv6** (config-std6-nacl)#	*page 4296*
IPv6 Access Control Policy	(config)#**ipv6 policy-class PRIVATEv6** (config-policy6-class)#	*page 4326*

DHCP Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
DHCPv4 Pool	(config)#**ip dhcp pool MyPool** (config-dhcp)#	*page 4336*
DHCPv6 Pool	(config)#**ipv6 dhcp pool MyPool** (config-dhcpv6)#	*page 4360*
DHCPv6 Server Pool	(config)#**ipv6 dhcp pool MYPOOL** (config-dhcpv6)#**host client-identifier F2A4C9** (config-dhcpv6-host)#	*page 4383*

Services Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Counter Profile	(config)#**counter-profile 0/1** (config-count-prof 0/1)#	*page 4391*
Desktop Auditing Local Policy	(config)#**desktop-auditing local-policy** (desktop-audit-policy)#	*page 4395*
Dynamic Counter	(config)#**dynamic-counter 0/1** (config-dyn-count 0/1)#	*page 4402*
Ethernet OAM CFM	(config)#**ethernet cfm domain domain1 level 6** (config-ecfm-domain)#	*page 4405*
Mail Agent	(config)#**mail-client myagent** (config-mail-client-myagent)#	*page 4423*
Network Sync	(config)#**network-sync** (config-ntwk-sync)#	*page 4434*
Over-Temperature Protection	(config)#**over-temperature protection** config-over-temp-protection)#	*page 4446*
Packet Capture	(config)#**packet-capture 1CAPTURE standard** (config-packet-capture-1CAPTURE)#	*page 4450*
QoS Map	(config)#**qos map VOICEMAP 10** (config-qos-map)#	*page 4464*
RADIUS Group	(config)#**aaa group server radius RADAuthgroup** (config-sg-radius)#	*page 4498*
Security Monitor	(config)#**ip security monitor** (config-secmon)#	*page 4503*
TACACS+ Group	(config)#**aaa group server tacacs+ TACAuthgroup** (config-sg-tacacs+)#	*page 4507*
Top Traffic	(config)#**ip flow top-talkers** (config-top-talkers)#	*page 4510*

Voice Command Sets

Voice Accounts Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Voice Line Account	(config)#**voice line sales** (config-sales)#	*page 4518*
Voice Loopback Account	(config)#**voice loopback 5555** (config-LB-5555)#	*page 4546*
Voice User Account	(config)#**voice user 4444** (config-4444)#	*page 4564*

Voice Groups Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Voice Call Pickup Group	(config)#**voice pickup-group Sales** (config-Sales)#	*page 4653*
Voice ISDN Group	(config)#**isdn-group 1** (config-isdn-group 1)#	*page 4656*
Voice Operator Group	(config)#**voice operator-group** (config-operator-group)#	*page 4664*
Voice Paging Group	(config)#**voice paging-group 8956** (config-8956)#	*page 4680*
Voice Ring Group	(config)#**voice ring-group 1234** (config-1234)#	*page 4685*
Voice Trunk Group	(config)#**voice grouped-trunk TestGroup** (config-TestGroup)#	*page 4704*

Voice Services Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Auto Attendant	(config)#**voice autoattendant Example 1212** (config-aa1212)#	*page 4715*
Call Coverage	(config)#**voice coverage Evening** (config-gch)#	*page 4718*
Call Queuing	(config)#**voice queue 6407** (config-6407)#	*page 4722*
FindMe-FollowMe Action Script	(config)#**voice user 4444** (config-4444)#**script Business** (config-4444-sc-Business)#	*page 4744*
FindMe-FollowMe Contact Group	(config)#**voice user 4444** (config-4444)#**contact-group 1** (config-4444-cg-1)#	*page 4752*

Command Set	Sample Access Path	For Full Command List, See...
Header Manipulation Rules (HMR)	(config)#**hmr policy POLICY1** (config-policy-POLICY1)#	*page 4762*
HMR Intercept	(config)#**hmr intercept** (config-hmr-intercept)#	*page 4812*
MGCP	(config)#**voice mgcp-endpoint 1** (config-mgcp-1)#	*page 4821*
Music on Hold	(config)#**voice music-on-hold player moh1** (config-moh1)#	*page 4853*
Proxy User Template	(config)#**ip sip proxy user-template Set1** (config-template-Set1)#	*page 4856*
SIP Proxy Monitor	(config)#**sip proxy sip-server monitor** Configuring New Proxy Monitor. (config-proxy-monitor)#	*page 4866*
SIP Server Monitor	(config)#**voice trunk t01 type sip** (config-T01)#**sip-server monitor** Configuring SIP Server Monitor. (config-sip-server-monitor)#	*page 4875*
SIP TLS Profile	(config)#**tls-profile TLSPROFILE1** (config-tls-profile-TLSPROFILE1)#	*page 4880*
SRTP Profile	(config)#**tls-profile SRTPPROFILE1** (config-srtp-profile-SRTPPROFILE1)#	*page 4888*
Voice CODEC List	(config)#**voice codec-list List1** (config-codec)#	*page 4893*
Voice CoS	(config)#**voice class-of-service set1** (config-cos-set1)#	*page 4897*
Voicemail CoS	(config)#**voice mail class-of-service class1** (config-vm-class1)#	*page 4936*
Voice Quality Monitoring Reporter	(config)#**ip rtp quality-monitoring reporter Reporter1** (config-rtp-reporter-Reporter1)#	*page 4945*

Voice Trunks Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Voice Analog Trunk DPT	(config)#**voice trunk t01 type analog supervision dpt** (config-t01)#	*page 4959*
Voice Analog Trunk Ground Start (GS)	(config)#**voice trunk t01 type analog supervision ground-start** (config-t01)#	*page 4959*

Command Set	Sample Access Path	For Full Command List, See...
Voice Analog Trunk Loop Start (LS)	(config)#**voice trunk t01 type analog supervision loop-start** (config-t01)#	*page 4959*
Voice ISDN Trunk	(config)#**voice trunk t01 type isdn** (config-t01)#	*page 5008*
Voice SIP Trunk	(config)#**voice trunk t01 type sip** (config-t01)#	*page 5052*
Voice T1 Trunk Feature Group D	(config)#**voice trunk t01 type t1-rbs supervision fgd role user** (config-t01)#	*page 5151*
Voice T1 Trunk Ground Start (GS)	(config)#**voice trunk t01 type t1-rbs supervision ground-start role user** (config-t01)#	*page 5151*
Voice T1 Trunk Immediate	(config)#**voice trunk t01 type t1-rbs supervision immediate role [network | user]** (config-t01)#	*page 5151*
Voice T1 Trunk	(config)#**voice trunk t01** (config-t01)#	*page 5151*
Voice T1 Trunk Loop Start (LS)	(config)#**voice trunk t01 type t1-rbs supervision loop-start role user** (config-t01)#	*page 5151*
Voice T1 Trunk Wink Role	(config)#**voice trunk t01 type t1-rbs supervision wink role [network | user]** (config-t01)#	*page 5151*

VPN Parameter Command Sets

Certificate Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
CA Profile	(config)#**crypto ca profile MyProfile** (ca-profile)#	*page 5209*
Certificate	(config)#**crypto ca certificate chain MyProfile** (config-cert-chain)#	*page 5221*

Crypto Map Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
Crypto Map IKE	(config)#**crypto map MapMap 10 ipsec-ike** (config-crypto-map)#	*page 5226*

Command Set	Sample Access Path	For Full Command List, See...
IPv4 Crypto Map Manual	(config)#**ip crypto map Map-Name 10 ipsec-manual** (config-crypto-map)#	*page 5244*
IPv6 Crypto Map Manual	(config)#**ipv6 crypto map Man-Name 10 ipsec-manual** (config-crypto6-map)#	*page 5254*
IPsec Profile	(config)#**ip crypto ipsec profile PROFILE1** (config-crypto-profile)#	*page 5260*

IKE Command Set Access Paths

Command Set	Sample Access Path	For Full Command List, See...
IKE Client	(config)#**crypto ike client configuration pool ConfigPool1** (config-ike-client-pool)#	*page 5270*
IKE Policy Attributes	(config)#**crypto ike policy 1** (config-ike)#**attribute 10** (config-ike-attribute)#	*page 5274*
IKE Policy	(config)#**crypto ike policy 1** (config-ike)#	*page 5280*

SYSTEM COMMAND SETS

This section includes the following command sets:

BASIC MODE COMMAND SET

To activate the Basic mode, simply log in to the unit. The following prompt displays:

>

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

exit on page 83

All other commands for this command set are described in this section in alphabetical order.

enable

Use the **enable** command (at the Basic Command mode prompt) to enter the Enable Command mode. Use the **disable** command to exit the Enable Command mode. Refer to *disable on page 482* for more information.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Functional Notes

The Enable Command mode provides access to operating and configuration parameters and should be password protected to prevent unauthorized use. Use the **enable password** command (found in the Global Configuration mode) to specify an Enable Command mode password. If the password is set, access to the Enable Commands (and all other “privileged” commands) is only granted when the correct password is entered. Refer to *enable password <password> on page 1270* for more information.

Usage Examples

The following example enters the Enable Command mode and defines an Enable Command mode password:

```
>enable
#configure terminal
(config)#enable password Adtran
```

At the next login, the following sequence must occur:

```
>enable
Password: ******
#
```


logout

Use the **logout** command to terminate the current session and return to the login screen.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the logout command being executed in the Basic mode:

```
>logout

Session now available

Press RETURN to get started.
```

ping

Use the **ping** command (at the Enable mode prompt) to verify IPv4 network connectivity. For information on how to verify IPv6 network connectivity, refer to *ping ipv6 on page 55*. Variations of this command include:

ping
ping [ip] <*ipv4 address* | *hostname*>
ping [ip] <*ipv4 address* | *hostname*> <*interface*>
ping [ip] <*ipv4 address* | *hostname*> **data** <*string*>
ping [ip] <*ipv4 address* | *hostname*> **df-bit [0 |1]**
ping [ip] <*ipv4 address* | *hostname*> **dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]**
ping [ip] <*ipv4 address* | *hostname*> **repeat** <*number*>
ping [ip] <*ipv4 address* | *hostname*> **size** <*value*>
ping [ip] <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
ping [ip] <*ipv4 address* | *hostname*> **timeout** <*value*>
ping [ip] <*ipv4 address* | *hostname*> **tos** <*value*>
ping [ip] <*ipv4 address* | *hostname*> **verbose**
ping [ip] <*ipv4 address* | *hostname*> **wait** <*interval*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> <*interface*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **data** <*string*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **df-bit [0 |1]**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **repeat** <*number*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **size** <*value*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **timeout** <*value*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **tos** <*value*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **verbose**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **wait** <*interval*>

After specifying the target IPv4 address to ping, the other parameters can be entered in any order. Use the **?** *after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

ip	Optional. Specifies an IPv4 ping.
<*interface*>	Optional. Specifies the egress interface when pinging an IPv4 address. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **ping** <*ipv4 address* | *hostname*> **?** to display a list of valid interfaces.

<ipv4 address | hostname>	Optional. Specifies the IPv4 address or host name of the system to ping. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Entering the **ping** command with no specified Internet Protocol version 4 (IPv4) address prompts the user with parameters for a more detailed **ping** configuration. Refer to *Functional Notes* (below) for more information.
data <*string*>	Optional. Specifies an alphanumerical string to use (the ASCII equivalent) as the data pattern in the ECHO_REQ packets.
df-bit 0	Optional. Specifies that the Don't Fragment (DF) bit in the IP header is not set.
df-bit 1	Optional. Specifies setting the DF bit in the IP header. This will prevent the ping packets from being fragmented along the way.
dscp	Optional. Specifies the differentiated services code point (DSCP) value.
<*value*>	Optional. Valid range is decimal **0** to **63**. The value can also be specified in hexadecimal by adding a **0x** prefix to the number.
af*xx*	Optional. Specifies the assured forwarding (AF) class and subclass for the DSCP value. Select from: 11 (001010), 12 (001100), 13 (001110), 21 (010010), 22 (010100), 23 010110), 31 (011010), 32 (011100), 33 (011110), 41 (100010), 42 (100100), or 43 (100110).
cs*x*	Optional. Specifies the class selector (CS) value for the DSCP value. Valid range for *x* is **0** to **7**.
default	Optional. Specifies default (000000) DSCP value.
ef	Optional. Specifies expedited forwarding (EF) (101110) for the DSCP value.
repeat <*number*>	Optional. Specifies the number of loopback messages to be sent. Range is **1** to **1024**.
size <*value*>	Optional. Specifies the datagram size (in bytes) of the ping packet. Valid range is **1** to **1448** bytes.
source <*ipv4 address*>	Optional. Specifies the IPv4 address to use as the source address in the ECHO_REQ (or interface) packets. The source IPv4 address must be a valid address local to the router on the specified virtual routing and forwarding (VRF) instance.
timeout <*value*>	Optional. Specifies the timeout period after which the ping is considered unsuccessful. Valid range is **1** to **60** seconds.
tos <*value*>	Optional. Specifies the type of service (ToS). The <*value*> can be specified as decimal (**0** to **255)** or as hexidecimal.
verbose	Optional. Enables detailed messaging.
vrf <*name*>	Optional. Specifies the VRF where the IPv4 address exists.
wait <*interval*>	Optional. Specifies a minimum time to wait between sending test packets. Valid range is **100** to **60000** milliseconds.

Default Values

By default, the **data** pattern is set to **abcd**.

By default, the **repeat** is set to **5**.

By default, the **size** value is set to **100** bytes.

By default, the **timeout** value is set to **2** seconds.

By default, the **wait** value is set to **100** milliseconds.

Command History

Release 1.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 17.2	Command was expanded to include the **verbose** and **wait** parameters, also changes were made to the **repeat** and **timeout** values.
Release 17.4	Command was expanded to include the **count** and **interval** parameters. The **repeat** and **wait** parameters were removed.
Release A4.01	Command was expanded to return the **wait** parameter.
Release 18.3	Command was expanded to include the optional **ip** and <*interface*> parameters.
Release R11.1.0	Functional Notes were enhanced to explain parameter behaviour with multiple entries.

Functional Notes

The **ping** command can be issued from both the Basic and Enable modes.

The **ping** command helps diagnose basic IPv4 network connectivity using the Packet Internet Groper program to repeatedly bounce Internet Control Message Protocol version 4 (ICMPv4) ECHO_REQ packets off a system (using a specified IPv4 address). AOS allows executing a standard **ping** request to a specified IP address, or provides a set of prompts to configure a more specific **ping** configuration.

After specifying the target IPv4 address (or hostname) to ping, the following parameters can be entered multiple times and in any order: **data**, **df-bit**, **repeat**, **size**, **source**, and **timeout**. When entering multiple instances of the same parameter, the last entry will be used. In the following example syntax, only the last entries for **data**, **repeat**, and **size** will be used, ignoring previous entries for these parameters:

ping ip 192.0.2.15 size 600 data bbbb repeat 3 size 300 data aaaa repeat 2 verbose dscp cs4 size 200

The following is a list of output messages from the **ping** command:

!	Success
-	Destination Host Unreachable
$	Invalid Host Address
X	TTL Expired in Transit
?	Unknown Host
*	Request Timed Out

The following is a list of available extended **ping** fields with descriptions:

Extended Commands	Specifies whether additional commands are desired for more ping configuration parameters. Answer yes (**y**) or no (**n**).
Source Address	Specifies the IPv4 address to use as the source address in the ECHO_REQ (or interface) packets.
Data Pattern	Specifies an alphanumerical string to use (the ASCII equivalent) as the data pattern in the ECHO_REQ packets.
Sweep Range of Sizes	Varies the sizes of the ECHO_REQ packets transmitted.
Sweep Min Size	Specifies the minimum size of the ECHO_REQ packet. Valid range is **0** to **1488**.
Sweep Max Size	Specifies the maximum size of the ECHO_REQ packet. Valid range is the sweep minimum size to **1448**.
Sweep Interval	Specifies the interval used to determine packet size when performing the sweep. Valid range is **1** to **1448**.
Verbose Output	Specifies an extended results output.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is an example of a successful **ping** command:

```
>ping
VRF Name [-default-]:
Target IP address:192.168.0.30
Repeat count [5]:5
Datagram Size [100]:100
Timeout in seconds [2]:2
Wait interval in milliseconds [100]:100
Extended Commands? [n]:n
Type CTRL+C to abort.
Legend: '!' = Success, '?' = Unknown host, '$' = Invalid host address
      '*' = Request timed out, '-' = Destination host unreachable
      'x' = TTL expired in transit, 'e' = Unknown error

Sending 5, 100-byte ICMP Echos to 192.168.0.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```


ping ethernet

Use the **ping ethernet** command to initiate a loopback message from one Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoint (MEP) to another MEP. These loopback messages are used to test the accessibility of the destination MEP. Variations of this command include:

ping ethernet <*target-mac-address* | *target-mep-id*>
ping ethernet <*target-mac-address* | *target-mep-id*> **count** <*number*>
ping ethernet <*target-mac-address* | *target-mep-id*> **data** <*pattern*>
ping ethernet <*target-mac-address* | *target-mep-id*> **domain** <*domain name*> **association** <*association name*>
ping ethernet <*target-mac-address* | *target-mep-id*> **domain none association** <*association name*>
ping ethernet <*target-mac-address* | *target-mep-id*> **drop-eligible**
ping ethernet <*target-mac-address* | *target-mep-id*> **interface** <*interface*>
ping ethernet <*target-mac-address* | *target-mep-id*> **mep** <*mep id*>
ping ethernet <*target-mac-address* | *target-mep-id*> **priority** <*priority*>
ping ethernet <*target-mac-address* | *target-mep-id*> **repeat** <*number*>
ping ethernet <*target-mac-address* | *target-mep-id*> **size** <*bytes*>
ping ethernet <*target-mac-address* | *target-mep-id*> **timeout** <*timeout*>
ping ethernet <*target-mac-address* | *target-mep-id*> **validate-data**
ping ethernet <*target-mac-address* | *target-mep-id*> **verbose**
ping ethernet <*target-mac-address* | *target-mep-id*> **wait** <*interval*>

After specifying the target for the loopback messages, the other parameters can be entered in any order.

Syntax Description

<*target-mac-address* | *target-mep-id*>	Specifies the destination for the loopback message. Medium access control (MAC) addresses are entered in the format **HH:HH:HH:HH:HH:HH**. Target MEP IDs are the unique numerical values identifying MEPs. MEP IDs range from **1** to **8191**.
count <*number*>	Optional. Specifies the number of loopback messages to send. Range is **1** to **1000000**.
data <*pattern*>	Optional. Specifies the pattern to be carried in the data time length value (TLV) of the loopback message. Pattern is up to four hexadecimal digits. Pattern range is **0** to **ffff**.
domain <*domain name*>	Optional. Specifies the maintenance domain to which the transmitting MEP belongs.
domain none	Optional. Specifies no maintenance domain.
association <*association name*>	Optional. Specifies the maintenance association to which the transmitting MEP belongs.

drop-eligible	Optional. Specifies the drop eligible bit value in the virtual local area network (VLAN) tag.
interface <*interface*>	Optional. Specifies the interface on which the transmitting MEP is configured. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.
mep <*mep id*>	Specifies the MEP ID of the transmitting MEP. MEP ID range is **1** to **8191**.
priority <*priority*>	Optional. Specifies the 802.1 priority bits that are sent in the loopback message. Range is **0** to **7**.
repeat <*number*>	Optional. Specifies the number of loopback messages to be sent. Range is **1** to **1024**.
size <*bytes*>	Optional. Specifies the size of the loopback message. Size ranges from **1** to **60** bytes.
timeout <*timeout*>	Optional. Specifies the time that the MEP will wait for a response to the loopback message. Range is **0** to **60** seconds.
validate-data	Optional. Specifies whether or not the transmitting MEP validates the contents of the data TLV in the received loopback messages.
verbose	Optional. Specifies that the results are in detailed, rather than summary, format.
wait <*interval*>	Optional. Specifies a minimum time to wait between sending loopback messages. Valid range is **100** to **60000** milliseconds.

Default Values

By default, the **count** value is set to **5**.

By default, the **data** pattern is set to **abcd**.

By default, the **drop-eligible** value is not set.

By default, the **interval** is set to **1000** milliseconds.

By default, the **priority** value is the priority specified in the MEP's configuration.

By default, the **size** value is set to **2** bytes.

By default, the **timeout** value is set to **2** seconds.

By default, the **validate-data** parameter is disabled.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface and the **wait** and **repeat** parameters.

Functional Notes

The **ping ethernet** command can be issued from both the Basic and Enable modes.

If the MEP ID is used as the target, the remote MEP must exist in the MEP continuity check message (CCM) database (meaning the remote MEP is transmitting valid CCMs) so that the MEP ID can be translated to the MAC address before the loopback message is transmitted.

Both the **domain** <*domain name*> and **association** <*association name*> parameters are not required if the source MEP ID of the MEP is specified and unique through the AOS device.

If the domain and association of the transmitting MEP are specified, and there is only one MEP in that domain or association, or if there is only one MEP configured on the unit, the **mep** <*mep id*> parameter is not required.

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

This command will not appear in the command line interface (CLI) unless Ethernet OAM CFM is enabled. To enable Ethernet OAM CFM, refer to the command ethernet cfm on page 1273.

Usage Examples

The following example initiates the Ethernet ping utility from an MEP in **Domain1** association **MA1** with a destination to an MEP with an MEP ID of **201**:

```
>ping ethernet 201 domain Domain1 association MA1
        Type CTRL+C to abort.
        Legend:    '!' = Success, '*' = Request timed out, 'd' = Data Mismatch
                   'o' = Out of order, '.' = No reply, 'e' = Unknown error.

        Sending 5, 100-byte LBRs to MEP 201 from MEP 1, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 202/668/1011 ms
```


ping ipv6

Use the **ping ipv6** command (at the Basic mode prompt) to verify IPv6 network connectivity. For information on how to verify IPv4 network connectivity, refer to *ping on page 48*. Variations of this command include:

ping ipv6 <*ipv6 address*>
ping ipv6 <*ipv6 address*> <*interface*>
ping ipv6 <*ipv6 address*> **data** <*string*>
ping ipv6 <*ipv6 address*> **destination-option**
ping ipv6 <*ipv6 address*> **hop-by-hop-option**
ping ipv6 <*ipv6 address*> **repeat** <*number*>
ping ipv6 <*ipv6 address*> **size** <*value*>
ping ipv6 <*ipv6 address*> **source** <*ipv6 address*>
ping ipv6 <*ipv6 address*> **timeout** <*value*>
ping ipv6 <*ipv6 address*> **verbose**
ping ipv6 <*ipv6 address*> **wait** <*interval*>
ping ipv6 vrf <*name*> <*ipv6 address*>
ping ipv6 vrf <*name*> <*ipv6 address*> <*interface*>
ping ipv6 vrf <*name*> <*ipv6 address*> **data** <*string*>
ping ipv6 vrf <*name*> <*ipv6 address*> **destination-option**
ping ipv6 vrf <*name*> <*ipv6 address*> **hop-by-hop-option**
ping ipv6 vrf <*name*> <*ipv6 address*> **repeat** <*interval*>
ping ipv6 vrf <*name*> <*ipv6 address*> **size** <*value*>
ping ipv6 vrf <*name*> <*ipv6 address*> **source** <*ipv6 address*>
ping ipv6 vrf <*name*> <*ipv6 address*> **timeout** <*value*>
ping ipv6 vrf <*name*> <*ipv6 address*> **verbose**
ping ipv6 vrf <*name*> <*ipv6 address*> **wait** <*interval*>

*After specifying the target IPv6 address to ping, the other parameters can be entered in any order. Use the **?** after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

<*interface*>	Specifies the egress interface when pinging an IPv6 link-local address (any address that has the prefix **FE80::/64**). Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **ping ipv6** <*ipv6 address*> **?** to display a list of valid interfaces. This variable is mandatory when pinging a link-local address. This variable is ignored when using a non-link-local address.
<*ipv6 address*>	Specifies the IPv6 address of the system to ping. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. Entering the **ping ipv6** command using a link-local destination address prompts the user for an egress interface.

data <*string*>	Optional. Specifies an alphanumerical string to use (the ASCII equivalent) as the data pattern in the ICMPv6 ECHO_REQ packets.
destination-option	Optional. Includes the destination option in the ICMPv6 ECHO_REQ packets.
hop-by-hop-option	Optional. Includes the hop-by-hop option in the ICMPv6 ECHO_REQ packets. This typically causes intermediate routers to process switch the packets, potentially detecting switching issues in these devices.
repeat <*number*>	Optional. Specifies the number of loopback messages to be sent. Range is **1** to **1024**.
size <*value*>	Optional. Specifies the datagram size (in bytes) of the ping packet. Valid range is **1** to **1448** bytes.
source <*ipv6 address*>	Optional. Specifies the IPv6 address to use as the source address in the ICMPv6 ECHO_REQ (or interface) packets. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. Entering the **ping ipv6** command using a link-local destination address prompts the user for an egress interface. The source IPv6 address must be a valid address local to the router on the specified virtual routing and forwarding (VRF) instance.
timeout <*value*>	Optional. Specifies the timeout period after which the ping is considered unsuccessful. Valid range is **1** to **60** seconds.
verbose	Optional. Enables detailed messaging.
vrf <*name*>	Optional. Specifies the VRF where the IPv6 address exists.
wait <*interval*>	Optional. Specifies a minimum time to wait between sending test packets. Valid range is **100** to **60000** milliseconds.

Default Values

By default, the **data** pattern is set to **abcd**.

By default, the **repeat** is set to **5**.

By default, the **size** value is set to **100** bytes.

By default, the **timeout** value is set to **2** seconds.

By default, the **wait** value is set to **100** milliseconds.

Command History

Release 18.1	Command was introduced.

Functional Notes

The **ping ipv6** command can be issued from both the Basic and Enable modes.

The **ping ipv6** command helps diagnose basic IPv6 network connectivity using the Packet Internet Groper program to repeatedly bounce Internet Control Message Protocol version 6 (ICMPv6) ECHO_REQ packets off a system (using a specified IPv6 address). AOS allows executing a standard **ping ipv6** request to a specified IPv6 address, or provides keywords to configure a more specific **ping ipv6** configuration.

The following is a list of output messages from the **ping ipv6** command:

!	Success
-	Destination Host Unreachable
$	Invalid Host Address
x	TTL Expired in Transit
?	Unknown Host
*	Request Timed out
e	Unknown Error
B	Packet too Big

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is example pings **2001:DB8:1A0::3** with **200** byte ICMPv6 ECHO_REQ packets:

>**ping ipv6 2001:DB8:1A0::3 size 200**
Type CTRL+C to abort.
Legend: '!' = Success, '?' = Unknown host, '$' = Invalid host address
'*' = Request timed out, '-' = Destination host unreachable
'x' = TTL expired in transit, 'e' = Unknown error
'B' = Packet too big

Sending 5, 200-byte ICMP Echos to 2001:DB8:1A0::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

ping stack-member <*number*>

Use the **ping stack-member** command to ping a member of the stack. Variations of this command include:

ping stack-member <*number*>
ping stack-member <*number*> **vrf** <*name*>

Syntax Description

<*number*>	Specified which member of the stack to ping.
vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) where the stack-member exists.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

The **ping stack-member** command can be issued from both the Basic and Enable modes.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example pings a member of the stack:

```
>ping stack-member 3
Type CTRL+C to abort.
Legend: '!' = Success, '?' = Unknown host, '$' = Invalid host address
      '*' = Request timed out, '-' = Destination host unreachable
      'x' = TTL expired in transit
Sending 5, 100-byte ICMP Echos to 169.254.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2.2/3 ms
#
```


ping twamp

Use the **ping twamp** command to execute a Two-Way Active Measurement Protocol (TWAMP) type ping to measure the packet loss, delay, and interpacket delay variation (IPDV) and display the results of the test. Use the subcommands in any combination, in any order, when specifying the destination site. Variations of this command include:

ping twamp
ping twamp <*ip address* | *hostname*>
ping twamp <*ip address* | *hostname*> **control-port** <*port*>
ping twamp <*ip address* | *hostname*> **data pattern**
ping twamp <*ip address* | *hostname*> **data pattern ascii** <*pattern*>
ping twamp <*ip address* | *hostname*> **data pattern hex** <*pattern*>
ping twamp <*ip address* | *hostname*> **data random**
ping twamp <*ip address* | *hostname*> **data zero**
ping twamp <*ip address* | *hostname*> **dscp** <*value*>
ping twamp <*ip address* | *hostname*> **interval** <*value*>
ping twamp <*ip address* | *hostname*> **port** <*port*>
ping twamp <*ip address* | *hostname*> **repeat** <*value*>
ping twamp <*ip address* | *hostname*> **size** <*value*>
ping twamp <*ip address* | *hostname*> **source** <*ip address*>
ping twamp <*ip address* | *hostname*> **source-port** <*port*>
ping twamp <*ip address* | *hostname*> **timeout** <*value*>
ping twamp <*ip address* | *hostname*> **verbose**
ping twamp <*ip address* | *hostname*> **wait** <*value*>
ping twamp vrf <*name*>
ping twamp vrf <*name*> <*ip address* | *hostname*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **control-port** <*port*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **data pattern**
ping twamp vrf <*name*> <*ip address* | *hostname*> **data pattern ascii** <*pattern*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **data pattern hex** <*pattern*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **data random**
ping twamp vrf <*name*> <*ip address* | *hostname*> **data zero**
ping twamp vrf <*name*> <*ip address* | *hostname*> **dscp** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **interval** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **port** <*port*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **repeat** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **size** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **source** <*ip address*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **source-port** <*port*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **timeout** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **verbose**

ping twamp vrf <*name*> <*ip address* | *hostname*> **wait** <*value*>

*The subcommands can be used in a string of any available combination. Use the **?** after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

<*ip address* | *hostname*>	Optional. Specifies the IP address or host name of the system to ping. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Entering the **ping twamp** command with no specified IP address prompts the user with parameters for a more detailed **ping twamp** configuration.
control-port <*port*>	Optional. Specifies the destination TWAMP control port. Port range is **1** to **65535**.
data	Optional. Specifies data used to pad packets. The following options are available:
pattern	Pads the packet with a user-specified pattern.
ascii <*pattern*>	Pads the packet with a user-specified ascii pattern.
hex <*pattern*>	Pads the packet with a user-specified hex pattern.
random	Pads the packet with random numbers.
zero	Pads the packet with all zeros.
dscp <*value*>	Optional. Specifies the differentiated services code point (DSCP) value. Valid range is **0** to **63**.
interval <*value*>	Optional. Specifies the interval between consecutive ping TWAMPs (in milliseconds). Valid range is **5** to **5000**.
port <*port*>	Optional. Specifies the destination port for the TWAMP test packets. Valid range is **1** to **65535**.
repeat <*value*>	Optional. Specifies the number of ping TWAMP packets. Valid range is **1** to **1000**.
size <*value*>	Optional. Specifies the datagram size. Valid range is **0** to **1462**.
source <*ip address*>	Optional. Specifies the source IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
source-port <*port*>	Optional. Specifies the source port for the TWAMP test packets. Valid range is **1** to **65535**.
timeout <*value*>	Optional. Specifies the timeout value in milliseconds. Valid range is **100** to **60000**.
verbose	Optional. Displays the detailed two-way ping verbose results for the specified IP address or host name.
vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) instance within which the ping is executed. If no VRF is specified, the default (unnamed) VRF is used.

wait <*value*>	Optional. Specifies the interval (in milliseconds) between consecutive TWAMP test packets. Range is **5** to **5000**.

Default Values

By default, the **data** is **zero,** the **dscp** is **0**, the **interval** value is **20,** the **port** value is **0,** the repeat value is **100**, the **size** is **0**, and the **timeout** is **2000** milliseconds.

Command History

Release 17.4	Command was introduced to replace the **twping** command.
Release 17.6	Command was expanded to include **control-port** and **wait** keywords.
Release A4.01	Command was expanded to include the **ascii** and **hex** pattern parameters.
Release R11.2.0	Command was expanded to include the **vrf** parameter.

Functional Notes

The **ping twamp** command can be issued from both the Basic and Enable modes.

Usage Examples

The following example executes a TWAMP ping:

```
>ping twamp
2009.06.03 11:18:24 IP.TWPING CTRL EVNT Attempting to connect
2009.06.03 11:18:24 IP.TWPING CTRL EVNT State changed Init -> Opening (event=Open Connection)
2009.06.03 11:18:24 IP.TWPING CTRL EVNT State changed Opening -> Setup (event=RX
    Server-Greeting)
2009.06.03 11:18:24 IP.TWPING CTRL EVNT State changed Setup -> Starting (event=TX
    Setup-Response)
2009.06.03 11:18:24 IP.TWPING CTRL PKT Sending Setup-Response (len=140)
 mode=1
 keyId=00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--MORE--
```

show clock

Use the **show clock** command to display the system time and date entered using the **clock set** command. Refer to *clock set <time> <day> <month> <year> on page 223* for more information.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example displays the current time and data from the system clock:

```
>show clock
23:35:07 UTC Tue Aug 20 2002
```


show snmp

Use the **show snmp** command to display the system Simple Network Management Protocol (SNMP) parameters and current status of SNMP communications.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is an example output using the **show snmp** command for a system with SNMP disabled and the default chassis and contact parameters:

```
>show snmp
Chassis: Chassis ID
Contact: Customer Service
0 Rx SNMP packets
  0 Bad community names
  0 Bad community uses
  0 Bad versions
  0 Silent drops
  0 Proxy drops
  0 ASN parse errors
```

show version

Use the **show version** command to display the current AOS version information.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is sample output from the **show version** command:

>**show version**

```
AOS version 06.01.00
 Checksum: 1F0D5243 built on Fri Nov 08 13:12:06 2002
 Upgrade key: de76efcfeb4c8eeb6901188475dd0917
Boot ROM version 03.00.18
 Checksum: 7A3D built on: Fri Nov 08 13:12:25 2002
Copyright (c) 1999-2002 Adtran Inc.
Serial number C14C6308

UNIT_2 uptime is 0 days 4 hours 59 minutes 43 seconds

System returned to ROM by Warm Start
Current system image file is "030018adv.biz"
Boot system image file is “030018adv.biz”
```


telnet *<ip address>*

Use the **telnet** command to open a Telnet session (through AOS) to another system on the network. Variations of this command include the following:

telnet *<ip address | hostname>*
telnet *<ip address | hostname>* **port** *<tcp port>*
telnet vrf *<name> <ip address | hostname>*
telnet vrf *<name> <ip address | hostname>* **port** *<tcp port>*

Syntax Description

<ip address | hostname>	Specifies the IP address or host name of the remote system. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal format (X:X:X:X::X). For example, **2001:DB8:1::1**.
port *<tcp port>*	Optional. Specifies the Transmission Control Protocol (TCP) port number to be used when connecting to a host through Telnet. Range is **1** to **65535**.
vrf *<name>*	Optional. Specifies the virtual routing and forwarding (VRF) where the IP address or host name exists.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 14.1	Command was expanded to specify the port number.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example opens a Telnet session with a remote system (**10.200.4.15**):

>**telnet 10.200.4.15**
User Access Login:
Password:

The following example opens a Telnet session with a remote system (**10.200.4.15**) on port **8010**:

>**telnet 10.200.4.15 port 8010**
User Access Login:
Password:

traceroute

Use the **traceroute** command to display the Internet Protocol version 4 (IPv4) routes a packet takes to reach the specified destination. Variations of this command include:

traceroute
traceroute [ip] <*ipv4 address* | *hostname*>
traceroute [ip] <*ipv4 address* | *hostname*> <*interface*>
traceroute [ip] <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
traceroute [ip] <*ipv4 address* | *hostname*> <*interface*> **source** <*ipv4 address*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> <*interface*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> <*interface*> **source** <*ipv4 address*>

Syntax Description

ip	Optional. Specifies an IPv4 trace.
<*interface*>	Optional. Specifies the egress interface to use for the trace. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **traceroute** <*ipv4 address* | *hostname*> **?** to display a list of valid interfaces.
<*ipv4 address* | *hostname*>	Optional. Specifies the IPv4 address or host name of the remote system's route to trace.
source <*ipv4 address*>	Optional. Specifies the IPv4 address of the interface to use as the source of the trace. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) where the route exists.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command was expanded to include the <*interface*> and **ip** parameters.

Functional Notes

The **traceroute** command can be issued from both the Basic and Enable modes.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **traceroute** command:

>**traceroute 192.168.0.1**
Type CTRL+C to abort.
Tracing route to 192.168.0.1 over a maximum of 30 hops
1 22ms 20ms 20ms 192.168.0.65
2 23ms 20ms 20ms 192.168.0.1

traceroute ethernet

Use the **traceroute ethernet** command to initiate a linktrace message from one Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoint (MEP) to another MEP. These linktrace messages are used to trace the packet route to a destination MEP. Variations of this command include:

traceroute ethernet <*target-mac-address* | *target-mep-id*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **domain** <*domain name*> **association** <*association name*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **domain none association** <*association name*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **fdb-only**
traceroute ethernet <*target-mac-address* | *target-mep-id*> **interface** <*interface*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **mep** <*mep id*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **sorted**
traceroute ethernet <*target-mac-address* | *target-mep-id*> **timeout** <*timeout*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **ttl** <*value*>

After specifying the target for the linktrace messages, the other parameters can be entered in any order.

Syntax Description

<*target-mac-address* | *target-mep-id*>	Specifies the destination for the linktrace message. Medium access control (MAC) addresses are entered in the format **HH:HH:HH:HH:HH:HH**. Target MEP IDs are the unique numerical values identifying MEPs. MEP IDs range from **1** to **8191**.
domain <*domain name*>	Optional. Specifies the maintenance domain to which the transmitting MEP belongs.
domain none	Optional. Specifies no maintenance domain.
association <*association name*>	Optional. Specifies the maintenance association to which the transmitting MEP belongs.
fdb-only	Optional. Specifies that the maintenance points on the route only use their forwarding database, and not their continuity check message (CCM) database when deciding if/how to forward linktrace messages.
interface <*interface*>	Optional. Specifies the interface on which the transmitting MEP is configured. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.

mep <*mep id*>	Optional. Specifies the MEP ID of the transmitting MEP. MEP ID range is **1** to **8191**.
sorted	Optional. Specifies the traceroute utility waits until all traceroute results have been received and sorted by hop count before displaying them.
timeout <*timeout*>	Optional. Specifies the time that the MEP will wait for a response to the linktrace message. Range is **0** to **60** seconds.
ttl <*value*>	Optional. Specifies the time to live (TTL) field of the linktrace message. Range is **0** to **255**.

Default Values

By default, the **timeout** value is set to **5** seconds.

By default, the **ttl** value is set to **5** seconds.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface and the Gigabit Switchport interface.

Functional Notes

The **traceroute ethernet** command can be issued from both the Basic and Enable modes.

If the MEP ID is used as the target, the remote MEP must exist in the MEP CCM database (meaning the remote MEP is transmitting valid CCMs) so that the MEP ID can be translated to the MAC address before the linktrace message is transmitted.

Both the **domain** <*domain name*> and **association** <*association name*> parameters are not required if the source MEP ID of the MEP is specified and unique through the AOS device.

If the domain and association of the transmitting MEP are specified, and there is only one MEP in that domain or association, or if there is only one MEP configured on the unit, the **mep** <*mep id*> parameter is not required.

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example initiates the Ethernet traceroute utility from a MEP with the ID **1** to an MEP with an MEP ID of **201**:

>**traceroute ethernet 201 mep 1**

```
Type CTRL+C to abort.

TTL 255. LTM Timeout is 5 seconds
Tracing route to        MEPID 201 (00:10:94:00:00:06)
                from    MEPID 1
                in      Domain_1/MA_1
MD Level 7, vlan 0
Traceroute sent via interface eth 0/1

-------------------------------------------------------------------------------------------------------------------------------
Hops    Mac                             Flags           Ingress-Action          Relay Action
          PrevHop                                               Egress-Action
-------------------------------------------------------------------------------------------------------------------------------
1       00:10:94:00:00:00               Forwarded       InNoTLV                 RLY_MPDB
            00:A0:C8:16:96:0D                                   EgOK
3       00:10:94:00:00:05               Forwarded       InNoTLV                 RLY_MPDB
            00:10:94:00:00:04                                   EgOK
2       00:10:94:00:00:04               Forwarded       InNoTLV                 RLY_MPDB
            00:10:94:00:00:00                                   EgOK
4       00:10:94:00:00:06 (Eg)          Terminal        InNoTLV                 RLY_HIT
            00:10:94:00:00:05

Destination reached
```

Remember that linktrace can be a tree-structure, and is not always linear. The PrevHop for Hop 3 in the previous example tells you the MAC of Hop 2. This gives you a way to trace the linktrace message when a tree-structure exists. Refer to Section J.5 of IEEE 802.1ag for more information.

traceroute ipv6

Use the **traceroute ipv6** command to display the IPv6 nodes traversed to reach the specified destination. Variations of this command include:

traceroute ipv6 *<ipv6 address>*
traceroute ipv6 *<ipv6 address> <interface>*
traceroute ipv6 *<ipv6 address> <interface>* **source** *<ipv6 address>*
traceroute ipv6 *<ipv6 address>* **source** *<ipv6 address>*
traceroute ipv6 vrf *<name> <ipv6 address>*
traceroute ipv6 vrf *<name> <ipv6 address> <interface>*
traceroute ipv6 vrf *<name> <ipv6 address> <interface>* **source** *<ipv6 address>*
traceroute ipv6 vrf *<name> <ipv6 address>* **source** *<ipv6 address>*

Syntax Description

<interface>	Optional. Specifies the egress interface when tracing a route to an IPv6 link-local address (any address that has the prefix **FE80::/64**). Interfaces are specified in the *<interface type> <slot/port* | *interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **traceroute ipv6** *<ipv6 address>* **?** to display a list of valid interfaces. This variable is ignored when using a non-link-local address.
<ipv6 address>	Specifies the IPv6 address of the remote system's route to trace. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. Entering the **traceroute ipv6** command using a link-local destination address prompts the user for an egress interface.
source *<ipv6 address>*	Optional. Specifies the IPv6 address to use as the source address in the probing packets. The source IPv6 address must be a valid address local to the router on the specified virtual routing and forwarding (VRF) instance.
vrf *<name>*	Optional. Specifies the VRF where the IPv6 address exists.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Functional Notes

The **traceroute ipv6** command can be issued from both the Basic and Enable modes.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS platforms supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **traceroute ipv6** command:

>**traceroute ipv6 2001:DB8:1A0::3**
Tracing route to over a maximum of 30 hops
Type CTRL+C to abort.
Legend: '!' = Success, '?' = Unknown host, '$' = Invalid host address
'*' = Request timed out, '-' = Destination host unreachable
'x' = TTL expired in transit, 'e' = Unknown error
'B' = Packet too big

1	2ms	2ms	3ms	2001:DB8:0:F820::5
2	102ms	109ms	102ms	2001:DB8:1A0::3

COMMON COMMANDS

The following section contains descriptions of commands that are common across multiple command sets. These commands are listed in alphabetical order.

alias “*<text>*”

Use the **alias** command to populate the ifAlias object identifier (OID) (Interface Table MIB of RFC 2863) for all physical and virtual interfaces when using Simple Network Management Protocol (SNMP) management stations. Use the **no** form of this command to remove an alias.

Syntax Description

“*<text>*”	Describes the interface (for SNMP) using an alphanumeric character string enclosed in quotation marks (limited to 64 characters).

Default Values

No default values are necessary for this command.

Applicable Command Modes

Applies to all interface mode command sets.

Command History

Release 1.1	Command was introduced.

Functional Notes

The ifAlias OID is a member of the ifXEntry object-type (defined in RFC 2863) used to provide a nonvolatile, unique name for various interfaces. This name is preserved through power cycles. Enter a string (using the **alias** command) which clearly identifies the interface.

Usage Examples

The following example defines a unique character string for the T1 interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#alias “CIRCUIT_ID_23-908-8887-401”**

Technology Review

Please refer to RFC 2863 for more detailed information on the ifAlias display string.

cross-connect

Use the **cross-connect** command to create a cross-connection between a created interfaces, whether virtual or physical. Interface connection types include connecting time division multiplexing (TDM) groups on an interface to a virtual interface, or connecting Point-to-Point Protocol (PPP) interfaces to Frame Relay interfaces for use with PPP over Frame Relay (PPPoFR), or PPP interfaces to Ethernet interfaces for PPP over Ethernet (PPPoE) functionality. Variations of this command include:

cross-connect *<number> <from interface> <to interface>*
cross-connect *<number> <from interface> <group number> <to interface>*

*Changing **cross-connect** settings could potentially result in service interruption.*

Syntax Description

<number>	Identifies the cross connection using a number descriptor or label (useful in systems that allow multiple cross connections). Valid range is **1** to **1024**.
<from interface>	Specifies the interface (physical or virtual) on one end of the cross connection. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; and for an ATM subinterface, use **atm 1.1**. Type **cross-connect 1 ?** for a list of valid interfaces.
<group number>	Optional. Specifies which configured TDM group to use for this cross connection. This subcommand only applies to T1 physical interfaces.
<to interface>	Specifies the virtual interface on the other end of the cross connection. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Use the **?** to display a list of valid interfaces.

Default Values

By default, there are no configured cross connections.

Applicable Command Modes

Applies to all interface mode command sets.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the E1 interface.
Release 17.7	Command was expanded to include its use with the PPPoFR feature.

Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release R10.6.0	Command was expanded to include the Ethernet and Gigabit Ethernet interfaces.

Functional Notes

Cross connections provide the mechanism for connecting a configured virtual (Layer 2) endpoint with a physical (Layer 1) interface. Supported Layer 2 protocols include Frame Relay, PPP, and PPPoE. This command can be used to connect the Frame Relay interface with a TDM group on a T1 circuit, to connect a PPP interface to a Frame Relay interface for use with PPPoFR encapsulation, and to connect a PPP interface with an Ethernet, Gigabit Ethernet, or MEF Ethernet interface. When using the **cross-connect** command to connect a Frame Relay endpoint to a T1 interface, the command is issued from the Frame Relay Interface Configuration mode or from the Global Configuration mode. When using the **cross-connect** command to link a PPP interface to a Frame Relay interface in PPPoFR, the command is issued from the PPP Interface Configuration mode. When using the **cross-connect** command to connect a PPP interface with an Ethernet, Gigabit Ethernet, or MEF Ethernet interface, the command is issued from the PPP Interface Configuration mode.

Usage Examples

The following example creates a Frame Relay endpoint and connects it to the T1 1/1 physical interface:

1. Create the Frame Relay virtual endpoint and set the signaling method:
   (config)**#interface frame-relay 1**
   (config-fr 1)**#frame-relay lmi-type cisco**

2. Create the subinterface and configure the PVC parameters (including DLCI and IP address):
   (config-fr 1)**#interface fr 1.1**
   (config-fr 1.1)**#frame-relay interface-dlci 17**
   (config-fr 1.1)**#ip address 168.125.33.252 255.255.255.252**

3. Create the TDM group of 12 DS0s (64K) on the T1 physical interface:
   (THIS STEP IS ONLY VALID FOR T1 INTERFACES.)
   (config)**#interface t1 1/1**
   (config-t1 1/1)**#tdm-group 1 timeslots 1-12 speed 64**
   (config-t1 1/1)**#exit**

4. Connect the Frame Relay subinterface with port T1 1/1:
   (config)**#cross-connect 1 t1 1/1 1 fr 1**

The following example creates a PPP interface and connects it to the Frame Relay interface for use with PPPoFR. The Frame Relay interface in this example is based on the interface configured in the previous example.

1. Create the PPP interface and enter its configuration mode:
   (config)**#interface ppp 1**
   (config-ppp 1)#

2. Configure the PPP interface (including IP address and PPP authentication information):
   (config-ppp 1)**#ip address 65.162.109.202 255.255.255.252**
   (config-ppp 1)**#ppp authentication chap**

(config-ppp 1)**#ppp chap hostname USERNAME**
(config-ppp 1)**#ppp chap password PASSWORD**
(config-ppp 1)**#no shutdown**

3. Connect the PPP interface with the Frame Relay interface:
(config-ppp 1)**#cross-connect 2 fr 1.1 ppp 1**

Technology Review

Creating an endpoint that uses a Layer 2 protocol (such as Frame Relay) is generally a four-step process:

Step 1:
Create the Frame Relay virtual endpoint (using the **interface frame-relay** command) and set the signaling method (using the **frame-relay lmi-type** command). Also included in the Frame Relay virtual endpoint are all the applicable Frame Relay timers logging thresholds, encapsulation types, etc. Generally, most Frame Relay virtual interface parameters should be left at their default state. For example, the following creates a Frame Relay interface labeled **7** and sets the signaling method to **ansi**.

(config)**#interface frame-relay 7**
(config-fr 7)**#frame-relay lmi-type ansi**

Step 2:
Create the subinterface and configure the permanent virtual circuit (PVC) parameters. Using the subinterface, apply access policies to the interface, create bridging interfaces, configure dial-backup, assign an IP address, and set the PVC data link connection identifier (DLCI). For example, the following creates a Frame Relay subinterface labeled **22,** sets the DLCI to **30,** and assigns an IP address of **193.44.69.253** to the interface.

(config-fr 7)**#interface fr 7.22**
(config-fr 7.22)**#frame-relay interface-dlci 30**
(config-fr 7.22)**#ip address 193.44.69.253 255.255.255.252**

Step 3: (VALID ONLY FOR T1 INTERFACES)
Specify the group of DS0s used for signaling on the T1 interface by creating a TDM group. Group any number of contiguous DS0s together to create a data pipe for Layer 2 signaling. Also use the **tdm-group** command to specify the per-DS0 signaling rate on the interface. For example, the following creates a TDM group labeled **9** containing 20 DS0s (each DS0 having a data rate of 56 kbps).

(config)**#interface t1 1/1**
(config-t1 1/1)**#tdm-group 9 timeslots 1-20 speed 56**
(config-t1 1/1)**#exit**

Step 4:
Make the association between the Layer 2 endpoint and the physical interface using the **cross-connect** command. Supported Layer 2 protocols include Frame Relay and Point-to-Point Protocol (PPP). For example, the following creates a cross-connect (labeled **5**) to make an association between the Frame Relay virtual interface (**fr 7**) and the TDM group configured on interface t1 1/1 (**tdm-group 9**).

(config)**#cross-connect 5 t1 1/1 9 fr 7**

The **cross-connect** command is also used by the PPP interface when using PPPoFR or PPPoE. PPPoFR can be used with a single T1 circuit, when using Multilink PPP, or when using Multilink Frame Relay. Configuration considerations vary according to the type of PPPoFR being used. For more information regarding PPPoFR, refer to the *PPPoFR Configuration Guide*. For more information regarding PPPoE, refer to the *Configuring the EFM NIM2 and the MEF Ethernet Interface* configuration guide. Both guides are available online at https://supportcommunity.adtran.com.

description *<text>*

Use the **description** command to identify the specified interface (for example, circuit ID, contact information, etc.). Use the **no** form of this command to remove a description.

Syntax Description

<text>	Identifies the specified interface using up to 80 alphanumeric characters.

Default Values

No default values are necessary for this command.

Applicable Command Modes

Applies to all interface mode command sets.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enters comment information using the **description** command:

(config)**#interface t1 1/1**
(config-t1 1/1)**#description This is the Dallas office T1**

do

Use the **do** command to execute any AOS command, regardless of the active configuration mode. It provides a way to execute commands in other modes without taking the time to exit the current mode and enter the desired one.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Applicable Command Modes

Applies to all mode command sets.

Command History

Release 2.1	Command was introduced.

Functional Notes

Use the **do** command to view configurations or interface states after configuration changes are made without exiting to the Enable mode.

Usage Examples

The following example shows the **do** command used to view the Frame Relay interface configuration while currently in the T1 Interface Configuration mode:

```
(config)#interface t1 1/1
(config-t1 1/1)#do show interfaces fr 7
fr 7 is ACTIVE
  Signaling type is ANSI signaling role is USER
  Polling interval is 10 seconds full inquiry interval is 6 polling intervals
Output queue: 0/0 (highest/drops)
    0 packets input 0 bytes
    0 pkts discarded 0 error pkts 0 unknown protocol pkts
    0 packets output 0 bytes
    0 tx pkts discarded 0 tx error pkts
```

end

Use the **end** command to exit the current configuration mode and enter the Enable Security mode.

*When exiting the Global Configuration mode, remember to perform a **copy running-config startup-config** to save all configuration changes.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Applicable Command Modes

Applies to all mode command sets except Basic mode.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the **end** command being executed in the T1 Interface Configuration mode:

```
(config-t1 1/1)#end
#
```

#- Enable Security mode command prompt

exit

Use the **exit** command to exit the current configuration mode and enter the previous one. For example, using the **exit** command in an interface configuration mode will activate the Global Configuration mode. When using the **exit** command in the Basic mode, the current session will be terminated.

*When exiting the Global Configuration mode, remember to perform a **copy running-config startup-config** to save all configuration changes.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Applicable Command Modes

Applies to all mode command sets.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the **exit** command being executed in the Global Configuration mode:

```
(config)#exit
#
```

#- Enable Security mode command prompt

interface

Use the **interface** command to activate the interface command set for the specified physical or virtual interface on an AOS unit. This command can be issued from the Global Configuration mode prompt or from any configuration mode to navigate to an interface configuration mode without issuing the **exit** command. The **interface** command is also used to create virtual interfaces prior to entering the configuration command set.

Type **interface ?** for a complete list of valid interface types on the unit. Refer to the command *interface range <interface type> <slot/port> - <slot/port> on page 1341* for more information. Use the **no** form of this command to delete a configured interface. Variations of this command include:

interface adsl <*slot/port*>
interface atm <*port* | *port.sublink*>
interface bri <*slot/port*>
interface bvi <*interface id*>
interface cellular <*slot/port*>
interface dds <*slot/port*>
interface demand <*interface id*>
interface demand <*interface id*> **encapsulation** [**hdlc** | **ppp**]
interface dot11ap <*ap* | *ap/radio* | *ap/radio.vap*> [**ap-type nv150** | **ap-type nv16x**] [**radio-type** [**802.11a** | **802.11bg**]]
interface e1 <*slot/port*>
interface ethernet <*slot/port* | *slot/port.subinterface*>
interface fdl <*slot/port*>
interface frame-relay <*port* | *port.sublink*>
interface fxo <*slot/port*>
interface fxs <*slot/port*>
interface gigabit-ethernet <*slot/port*>
interface gigabit-switchport <*slot/port*>
interface hdlc <*interface id*>
interface hssi <*slot/port*>
interface loopback <*interface id*>
interface mef-ethernet <*slot/port* | *slot/port.subinterface*>
interface modem <*slot/port*>
interface port-channel <*interface id*>
interface ppp <*interface id*>
interface pri <*slot/port*>
interface serial <*slot/port*>
interface sdsl <*slot/port*>
interface shdsl <*slot/port*>
interface switchport <*slot/port*>
interface t1 <*slot/port*>
interface t3 <*slot/port*>
interface t4 <*slot/port*>
interface tunnel <*interface id*> [**gre ip** | **multipoint-gre ip** | **vxlan**]
interface vdsl <*slot/port*>

interface vlan <*interface id*>
interface xgigabit-switchport <*slot/port*>

Syntax Description

adsl <*slot/port*>	Identifies physical asymmetric digital subscriber line (ADSL) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface adsl ?** for information regarding valid ranges.
atm <*port* | *port.sublink*>	Identifies and creates asynchronous transfer mode (ATM) virtual interfaces or subinterfaces. Port number range is **1** to **1024**. Sublink number range is **1** to **65535**.
bri <*slot/port*>	Identifies physical basic rate interfaces (BRIs). Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface bri ?** for information regarding valid ranges.
bvi <*interface id*>	Identifies bridged virtual interfaces (BVIs). This ID must correspond to an existing bridge group. Valid range is **1** to **255**.
cellular <*slot/port*>	Identifies physical cellular interfaces. Slot numbers are either 0 or 1. Port numbers begin at 1 with a range dependent on the unit.
dds <*slot/port*>	Identifies physical digital data service (DDS) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface dds ?** for information regarding valid ranges.
demand <*interface id*>	Identifies and creates virtual demand routing interfaces. Valid range is **1** to **1024**.
encapsulation [**hdlc** | **ppp**]	Optional. Specifies the encapsulation type for the demand routing interface. The **hdlc** encapsulation type specifies high level data link control (HDLC) encapsulation, and the **ppp** encapsulation type specifies Point-to-Point Protocol (PPP) encapsulation. If no encapsulation type is specified, PPP encapsulation is used for the demand routing interface by default.
dot11ap <*ap* | *ap/radio* | *ap/radio.vap*>	Identifies wireless access point, radio, and/or virtual access point (VAP) interfaces. The AP number range is **1** to **8**. The radio is either 1 or 2. The VAP number range is **1** to **8**.
ap-type nv150	Specifies the wireless access point (AP) type as a NetVanta 150.
ap-type nv16x	Specifies the wireless AP type as a NetVanta 160 Series.
radio-type [**802.11a** | **802.11bg**]	Specifies the radio interface type. Valid interface types are **802.11a** and **802.11bg**.
e1 <*slot/port*>	Identifies physical E1 interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface e1 ?** for information regarding valid ranges.
ethernet <*slot/port*>	Identifies physical Ethernet interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface ethernet ?** for information regarding valid ranges.

fdl <*slot/port*>	Identifies physical facility data link (FDL) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface fdl ?** for information regarding valid ranges.
frame-relay <*port* | *port.sublink*>	Identifies and creates virtual Frame Relay interfaces. Port number range is **1** to **1024**. Sublink range is **1** to **1007**.
fxo <*slot/port*>	Identifies physical foreign exchange office (FXO) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface fxo ?** for information regarding valid ranges.
fxs <*slot/port*>	Identifies physical foreign exchange station (FXS) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface fxs ?** for information regarding valid ranges.
gigabit-ethernet <*slot/port*>	Identifies physical gigabit Ethernet interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface gigabit-ethernet ?** for information regarding valid ranges.
gigabit-switchport <*slot/port*>	Identifies physical gigabit switchport interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface gigabit-switchport ?** for information regarding valid ranges.
hdlc <*interface id*>	Identifies and creates virtual high level data link control (HDLC) interfaces. Valid range is **1** to **1024**.
hssi <*slot/port*>	Identifies physical high speed serial interfaces (HSSIs). Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface hssi ?** for information regarding valid ranges.
loopback <*interface id*>	Identifies and creates virtual loopback interfaces. Valid range is **1** to **1024**.
mef-ethernet <*slot/port*>	Identifies physical Metro Ethernet Forum (MEF) Metro Ethernet interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit.
modem <*slot/port*>	Identifies physical analog modem interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface modem ?** for information regarding valid ranges.
port-channel <*interface id*>	Creates and configures virtual link aggregation interfaces. Valid range is **1** to **6**.
ppp <*interface id*>	Identifies and creates virtual Point-to-Point Protocol (PPP) interfaces. Valid range is **1** to **1024**.
pri <*slot/port*>	Identifies physical primary rate interfaces (PRIs). Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface pri ?** for information regarding valid ranges.

serial <*slot/port*>	Identifies physical serial ports. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface serial ?** for information regarding valid ranges.
sdsl <*slot/port*>	Identifies physical symetric digital subscriber line (SDSL) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface sdsl ?** for information regarding valid ranges.
shdsl <*slot/port*>	Identifies physical single-pair high-speed digital subscriber line (SHDSL) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface shdsl ?** for information regarding valid ranges.
switchport <*slot/port*>	Identifies physical switchport interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface switchport ?** for information regarding valid ranges.
t1 <*slot/port*>	Identifies physical T1 interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface t1 ?** for information regarding valid ranges.
t3 <*slot/port*>	Identifies physical T3 interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface t3 ?** for information regarding valid ranges.
t4 <*slot/port*>	Identifies physical T4 interface. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface t4 ?** for information regarding valid ranges.
ttunnel <*interface id*>	Identifies the tunnel interface ID. Valid range is **1** to **1024**.
gre ip	Creates a virtual Internet Protocol version 4 (IPv4) generic routing encapsulation (GRE) tunnel interface.
multipoint-gre ip	Creates a virtual IPv4 GRE multipoint tunnel interface.
vxlan	Creates a virtual extensible local area network (VxLAN) tunnel interface.
vdsl <*slot/port*>	Identifies physical very high-speed digital subscriber line (VDSL) interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface vdsl ?** for information regarding valid ranges.
vlan <*interface id*>	Identifies and creates virtual local area network (VLAN) interfaces. Valid range is **1** to **4094**.
xgigabit-switchport <*slot/port*>	Identifies physical 10-gigabit switchport interfaces. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **interface xgigabit-switchport ?** for information regarding valid ranges.

Default Values

By default, an interface is inactive. To activate the interface, enter the **no shutdown** command from within the specific interface command set; for example, (config-ppp 7)**#no shutdown**. There are no default values for these commands.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was expanded to include the loopback interface.
Release 8.1	Command was expanded to include the ATM interface.
Release 9.1	Command was expanded to include the HDLC interface.
Release 11.1	Command was expanded to include demand, FXO, and PRI interfaces.
Release 15.1	Command was expanded to allow navigation from one interface to another without exiting the current configuration mode. Also, expanded to include AP, radio, VAP, and BVI interfaces.
Release 17.2	Command was expanded to include cellular interface.
Release A4.01	Command was expanded to include the MEF Metro Ethernet interface.
Release 18.1	Command was expanded to include the **ap-type** and **radio-type** parameters.
Release R10.1.0	The **tunnel** <*interface id*> command was changed to **tunnel** <*interface id*> **gre ip**.
Release R10.4.0	Command was expanded to include the NetVanta 160 Series AP type (**ap-type nv16x**).
Release R10.8.0	Command was expanded to include the **encapsulation** [**hdlc** | **ppp**] parameter on the demand routing interface.
Release R10.10.0	Command was expanded to include the SDSL, VDSL, and 10 gigabit switchport interfaces.
Release R10.11.0	Command was expanded to include the T4 interface.
Release R13.1.0	The **tunnel** <*interface id*> command was expanded to include **vxlan** parameter.

Functional Notes

When identifying a physical interface slot and port, keep the following in mind:

- Built-in nonremovable interfaces are identified by slot 0.
- Removable interfaces are identified by the physical labels on the slots.
- Interfaces are numbered per slot, from left to right, starting with 1.

Usage Examples

The following example uses the **interface** command to navigate from the T1 Interface Configuration mode to a Frame Relay interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#interface fr 7**
(config-fr 7)#

The following examples activate the interface configuration mode for the specified interface type:

For an ADSL interface:

(config)**#interface adsl 1/1**
(config-adsl 1/1)#

For an ATM subinterface:

(config)**#interface atm 1.1**
(config-atm 1.1)#

For a BRI interface:

(config)**#interface bri 1/2**
(config-bri 1/2)#

For a BVI interface:

(config)**#bridge irb**
(config)**#interface bvi 1**
(config-bvi 1)#

For a cellular interface:

(config)**#interface cellular 1/1**
(config-cellular 1/1)#

For a DDS interface:

(config)**#interface dds 1/1**
(config-dds 1/1)#

For a demand routing interface using HDLC encapsulation:
(config)**#interface demand 1 encapsulation hdlc**
(config-demand 1)#

For a dot11ap interface:

(config)**#interface dot11ap 1**
(config-dot11ap 1)#

For an E1 interface:

(config)**#interface e1 1**
(config-e1 1)#

For an Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)#

For an Ethernet subinterface:

(config)**#interface eth 0/1.1**
(config-eth 0/1.1)#

For an FDL interface:

(config)**#interface fdl 1/1**
(config-fdl 1/1)#

For a Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)#

For an FXO interface:

(config)**#interface fxo 0/1**
(config-fxo 0/1)#

For an FXS interface:

(config)**#interface fxs 2/1**
(config-fxs 2/1)#

For a Gigabit Ethernet interface:

(config)**#interface gigabit-ethernet 0/3**
(config-giga-eth 0/3)#

For an HDLC interface:

(config)**#interface hdlc 1**
(config-hdlc 1)#

For an HSSI interface:

(config)**#interface hssi 1/1**
(config-hssi 1/1)#

For a loopback interface:

(config)**#interface loopback 8**
(config-loop 8)#

For an MEF Ethernet interface:

(config)**#interface mef-ethernet 2/1**
(config-mef-ethernet 2/1)#

For a modem interface:

(config)**#interface modem 1/1**
(config-modem 1/1)#

For a port channel interface:

(config)**#interface port-channel 6**
Creating Port Channel interface 6.
(config-p-chan6)#

For a PPP interface:

(config)**#interface ppp 100**
(config-ppp 100)#

For a PRI interface:

(config)**#interface pri 2**
(config-pri 2)#

For a serial interface:

(config)**#interface serial 1/1**
(config-serial 1/1)#

For an SDSL interface:

(config)**#interface sdsl 1/1**
(config-sdsl 1/1)#

For an SHDSL interface:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)#

For a switchport interface:

(config)**#interface switchport 0/2**
(config-swx 0/2)#

For a 10 gigabit switchport interface:

(config)**#interface xgigabit-switchport 1/1**
(config-xgiga-swx 1/1)#

For a T1 interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#**

For a T3 interface:

(config)**#interface t3 1/1**
(config-t3 1/1)**#**

For a T4 interface:

(config)**#interface t4 1/1**
(config-t4 1/1)**#**

For a tunnel interface:

(config)**#interface tunnel 300 gre ip**
(config-tunnel 300)**#**

For a VDSL interface:

(config)**#interface vdsl 1/1**
(config-vdsl 1/1)**#**

For a VLAN interface:

(config)**#interface vlan 300**
(config-vlan 300)**#**

For a wireless access point:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#**

shutdown

Use the **shutdown** command to disable an interface (both physical and virtual) or an Adtran Operating System (AOS) feature. Use the **no** form of this command to turn on the interface or enable the feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are disabled.

The default setting for feature commands vary. Refer to the individual feature command set for specific details about feature default settings.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **shutdown** command applies to all interface mode command sets and certain feature command sets.

When the **shutdown** command is issued from within an interface configuration command set, it disables the interface so no traffic will be passed through. When the **shutdown** command is issued from within a feature command set, it disables the feature and causes it to stop functioning. Using this command allows you to temporarily disable an interface or feature without altering the configurationg settings related to it. Once the **no shutdown** command is issued, the interface or feature is enabled, resuming functionality using the previously configured settings.

Usage Examples

The following example administratively disables the modem interface:

(config)**#interface modem 1/2**
(config-modem 1/2)**#shutdown**

The following example disables the packet capture feature:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#shutdown**

ENABLE MODE COMMAND SET

To activate the Enable mode, enter the **enable** command at the Basic mode prompt. (If an enable password has been configured, a password prompt will display.) For example:

```
>enable
Password: XXXXXXX
#
```

In AOS Release 17.1, output modifiers were introduced for all **show** commands. These modifiers help specify the information displayed in the **show** command output. The modifiers are appended to the end of the **show** command, preceded by the pipe character (|), and followed by the *<text>* to **exclude**, **include**, or with which to **begin** the display. The following output modifiers are common for all **show** commands:

| begin *<text>*	Produces output that begins with lines, including the specified text and every line thereafter.
| exclude *<text>*	Produces output that excludes any lines containing the specified text.
| include *<text>*	Produces output that only displays lines with the specified text.

In the following example, the **show** command was modified to **begin** its display with the lines **http server** and display all lines thereafter:

```
#show run | begin ip http server
no http server
no http secure-server
no snmp agent
no ip ftp server
ip ftp server default-filesystem flash
no ip scp server
no ip sntp server
!
```

In the following example, the **exclude** modifier was used with the **show** command to exclude lines of text containing the words **no shutdown**:

```
#show run interface ppp 1 | exclude no shutdown
!
!
interface ppp 1
ip address 10.2.0.1 255.255.255.0
ip access-policy UNTRUSTED
crypto map SITE2SITE
no lldp send-and-receive
cross-connect 1 t1 1/1 1 ppp 1
!
```


In the following example, the **include** modifier was used with the **show** command to only display information about interfaces:

```
#show run | include interface
interface switchport 0/1
interface switchport 0/2
interface switchport 0/3
interface switchport 0/4
interface switchport 0/5
interface switchport 0/6
interface switchport 0/7
--MORE--
```

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

exit on page 83

All other commands for this command set are described in this section in alphabetical order.

application

Use the **application** command to enter the application command set. Ethernet Y.1731 and network synchronization (Network Sync) can be configured from this set. Available Ethernet Y.1731 commands in the application set include:

ethernet y1731 meg char-string *<name> <level> <id>*
ethernet y1731 meg icc-umc *<name> <level> <id>*

Syntax Description

char-string *<name>*	Specifies a Y.1731 maintenance entity group (MEG) name using a character string format. Maximum length is **45** ASCII characters.
icc-umc *<name>*	Specifies a Y.1731 MEG name using the ITU-CarrierCode Unique MEG ID Code MEG (ICC-UMC) format. Maximum length is **13** ASCII characters.
<level>	Specifies the MEG level. Valid range is **0** to **7**.
<id>	Specifies the MEG ID. Valid range is **1** to **8191**.

Default Values

By default, no Y.1731 applications are configured. By default, no Network Sync applications are configured.

Command History

Release R10.10.0	Command was introduced.
Release R10.11.0	Command was expanded to include Network Sync configuration commands.

Functional Notes

The Y.1731 application is configured using the commands outlined in *Y.1731 Application Command Set on page 1997*.

The Network Sync application is configured using the commands outlined in *Network Sync Application Command Set on page 1992*.

Usage Examples

The following example access the application command set:

```
>enable
#application
(app)#
```


The following example accesses the Y.1731 application command set:

>**enable**
#application
(app)**#ethernet y1731 meg char-string MEG1 3 100**
(app-y1731 100)#

auto-config restart

Use the **auto-config restart** command to restart the AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at *https://supportcommunity.adtran.com*.

> NOTE *To stop AOS automatic self-configuration once it has started, enter the **no auto-config** command from the Global Configuration Mode prompt. The AOS automatic self-configuration feature must be disabled before the **auto-config restart** command will start the process.*

Syntax Description

No subcommands.

Default Values

There is no default setting for this command.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was relocated to the Enable Mode from the Global Configuration Mode.

Usage Examples

The following command restarts the automatic configuration process:

```
>enable
#auto-config restart
```


boot config

Use the **boot config** command to modify system boot parameters by specifying the location and name of primary and secondary configuration files. Use the **no** form of this command to use the default startup configuration file. Variations of this command include:

boot config cflash <*primary filename*>
boot config cflash <*primary filename*> **cflash** <*secondary filename*>
boot config cflash <*primary filename*> **flash** <*secondary filename*>
boot config flash <*primary filename*>
boot config flash <*primary filename*> **cflash** <*secondary filename*>
boot config flash <*primary filename*> **flash** <*secondary filename*>

*The **cflash** parameter is only valid for units with CompactFlash® capabilities.*

Syntax Description

cflash	Specifies that the configuration file is located in CompactFlash memory.
flash	Specifies that the configuration file is located in flash memory.
<*primary filename*>	Specifies the name of the primary configuration file (file names are case sensitive).
<*secondary filename*>	Optional. Specifies the name of the backup configuration file.

Default Values

No default values are necessary for this command.

Command History

Release 18.2	Command was introduced

Usage Examples

The following example specifies the file **myconfig.biz** (located in flash memory) as the primary system boot file:

>**enable**
(config)**#boot config flash myconfig.biz**

The following example specifies the file **myconfig.biz** (located in flash memory) as the primary system boot file and the file **mybackupconfig.biz** (located in CompactFlash memory) as the backup configuration file:

>**enable**
(config)**#boot config flash myconfig.biz cflash mybackupconfig.biz**

boot system

Use the **boot system** command to specify the system image loaded at startup. Variations of this command include:

boot system cflash <*primary filename*>
boot system cflash <*primary filename*> **verify**
boot system cflash <*primary filename*> **cflash** <*secondary filename*>
boot system cflash <*primary filename*> **cflash** <*secondary filename*> **verify**
boot system cflash <*primary filename*> **flash** <*secondary filename*>
boot system cflash <*primary filename*> **flash** <*secondary filename*> **verify**
boot system cflash <*primary filename*> **no-backup**
boot system cflash <*primary filename*> **no-backup verify**
boot system flash <*primary filename*>
boot system flash <*primary filename*> **verify**
boot system flash <*primary filename*> <*secondary filename*>
boot system flash <*primary filename*> <*secondary filename*> **verify**
boot system flash <*primary filename*> **cflash** <*secondary filename*>
boot system flash <*primary filename*> **cflash** <*secondary filename*> **verify**
boot system flash <*primary filename*> **flash** <*secondary filename*>
boot system flash <*primary filename*> **flash** <*secondary filename*> **verify**
boot system flash <*primary filename*> **no-backup**
boot system flash <*primary filename*> **no-backup verify**

*The **cflash** parameter is only valid for units with CompactFlash® capabilities.*

*For units without CompactFlash capabilities, the secondary media type does not need to be specified. Refer to the last example under **Usage Examples**.*

Syntax Description

cflash	Specifies the system image is located in CompactFlash memory.
flash	Specifies the system image is located in flash memory.
no-backup	Specifies that there is no backup image present.
<*primary filename*>	Specifies the file name of the image (file names are case sensitive). Image files should have a .biz extension.
<*secondary filename*>	Specifies a name for the backup image.
verify	Optional. Verifies the image checksum.

Default Values

No default values are necessary for this command.

Command History

Release 18.2	Command was introduced.
Release R12.1.0	Command version **boot system flash** was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

Detailed instructions for upgrading AOS and loading files into flash memory are found online at http://supportforums.adtran.com.

The **boot system flash** command is not available in vAOS instances.

Usage Examples

The following example specifies **myimage.biz** (located in CompactFlash memory) as the primary image file with no backup image:

```
>enable
#boot system cflash myimage.biz no-backup
```

The following example specifies **myimage.biz** (located in flash memory) as the primary image file with no backup image:

```
>enable
#boot system flash myimage.biz no-backup
```

The following example specifies **myimage.biz** (located in flash memory) as the primary image file and **mybackupimage.biz** (also located in flash memory) as the backup image:

```
>enable
#boot system flash myimage.biz mybackupimage.biz
```

clear activchassis

Use the **clear activchassis** command to cause the master device to trigger a restart of the ActivChassis supervision protocols. This action causes the entire ActivChassis to restart discovery and to re-resolve the current ActivChassis configuration.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release AC1.0	Command was introduced.

Usage Examples

The following example restarts the ActivChassis supervision protocols:

```
>enable
#clear activchassis
```


clear arp-cache

Use the **clear arp-cache** command to remove all dynamic entries from the Address Resolution Protocol (ARP) cache table. Variations of this command include:

clear arp-cache
clear arp-cache vrf <*name*>

Syntax Description

vrf <*name*>	Optional. Clears the ARP cache entry for a specific virtual routing and forwarding (VRF).

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release A1	Command was expanded to include the **vrf** parameter.

Usage Examples

The following example removes all dynamic entries from the ARP cache:

>**enable**
#clear arp-cache

clear arp-entry <*ip address*>

Use the **clear arp-entry** command to remove a single entry from the Address Resolution Protocol (ARP) cache. Variations of this command include:

clear arp-entry <*ip address*>
clear arp-entry <*ip address*> **vrf** <*name*>

Syntax Description

<*ip address*>	Specifies a valid IP address to remove. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrf <*name*>	Optional. Clears the ARP entry for a specific virtual routing and forwarding (VRF).

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release A1	Command was expanded to include the **vrf** parameter.

Usage Examples

The following example removes the entry for 10.10.10.1 from the ARP cache:

>**enable**
#clear arp-entry 10.10.10.1

clear bgp

Use the **clear bgp** command to clear information for Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP). You can clear BGP neighbors, BGP IPv4 and IPv6 route information, and BGP connections on the default or nondefault virtual routing and forwarding (VRF) instances. Variations of this command include:

clear bgp * [mef-ethernet <*slot/port*> **| system-control-evc** | **system-management-evc]**
clear bgp <*number*> **[system-control-evc** | **system-management-evc]**
clear bgp <*ipv4 address*> **[system-control-evc** | **system-management-evc]**
clear bgp <*ipv6 address*> **[system-control-evc** | **system-management-evc]**
clear bgp any-vrf [* | <*number*> **|** <*ipv4 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in | out | soft]**
clear bgp any-vrf [* | <*number*> | <*ipv6 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**
clear bgp any-vrf ipv4 [* | <*number*> | <*ipv4 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**
clear bgp any-vrf ipv6 [* | <*number*> | <*ipv6 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**
clear bgp ipv4 [* | <*number*> | <*ipv4 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**
clear bgp ipv6 [* | <*number*> | <*ipv6 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**
clear bgp vrf <*name*> **[*** | <*number*> | <*ipv4 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**
clear bgp vrf <*name*> **ipv4 [*** | <*number*> | <*ipv4 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**
clear bgp vrf <*name*> **ipv6 [*** | <*number*> | <*ipv6 address*>**] [mef-ethernet** <*slot/port*> **| system-control-evc** | **system-management-evc] [in** | **out** | **soft]**

Syntax Description

*****	Clears all BGP neighbors.
<*number*>	Clears all BGP neighbors with the specified autonomous system (AS) number. Range is **1** to **4294967295**.
<*ipv4 address*>	Clears the BGP neighbor with the specified IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*ipv6 address*>	Clears the BGP neighbor with the specified IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (for example, **2001:DB8:1::1**).
any-vrf	Optional. Clears BGP connections for all VRF instances.
ipv4	Optional. Clears all BGP IPv4 route information.
ipv6	Optional. Clears all BGP IPv6 route information.
in	Causes a *soft* reset inbound with a neighbor, reprocessing routes advertised by that neighbor.

out	Causes a *soft* reset outbound with a neighbor, resending advertised routes to that neighbor.
soft	Causes a *soft* reset both inbound and outbound.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.
vrf <*name*>	Optional. Clears connections for a nondefault VRF instance.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 18.1	Command was altered to support 4-byte AS number (previously AOS only supported 2-byte numbers).
Release 18.3	Command syntax was changed to remove the **ip** keyword for Adtran internetworking products. In addition, the **any-vrf**, **vrf** <*name*>, and **ipv4** parameters were added.
Release R10.1.0	Command was expanded to include IPv6 BGP capability, and the **ipv6** and <*ipv6 address*> parameters were added. In addition, the command syntax was changed to remove the **ip** keyword for Adtran voice products.
Release R.10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

The **clear bgp** command must be issued to re-initialize the BGP process between the peers matching the given arguments. Most neighbor changes, including changes to prefix-list filters, do not take effect until the **clear** command is issued. A hard reset clears the Transmission Control Protocol (TCP) connection with the specified peers, which results in clearing the table. This method of clearing is disruptive and causes peer routers to record a route flap for each route.

The **out** version of this command provides a soft reset out to occur by causing all routes to be re-sent to the specified peer(s). TCP connections are not torn down, so this method is less disruptive. Output filters/policies are re-applied before sending the update.

The **in** version of this command provides a soft reset in to occur by allowing the router to receive an updated table from a peer without tearing down the TCP connection. This method is less disruptive and does not count as a route flap. Currently, all of the peer's routes are stored permanently, even if they are filtered by a prefix list. The command causes the peer's routes to be reprocessed with any new parameters.

Usage Examples

The following example causes a hard reset with peers with an AS number of 101:

>**enable**
#clear bgp 101

clear bridge <*number*>

Use the **clear bridge** command to clear all counters associated with bridging (or for a specified bridge group). Variations of this command include:

clear bridge
clear bridge <*number*>

Syntax Description

<*number*>	Optional. Specifies a single bridge group. Range is **1** to **255**.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example clears all counters for bridge group 17:

>**enable**
#clear bridge 17

clear buffers max-used

Use the **clear buffers max-used** command to clear the maximum-used statistics for buffers displayed in the **show memory heap** command.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example clears the maximum-used buffer statics:

```
>enable
#clear buffers max-used
```

clear counters *<interface>*

Use the **clear counters** command to clear the counters for a specified interface or Ethernet virtual connection (EVC). Variations of this command include:

clear counters evc *<name>*
clear counters *<interface>*

Syntax Description

evc *<name>*	Specifies an EVC on which to clear counters.
<interface>	Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear counters ?** or **show interfaces ?** for a complete list of interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface and the gigabit switchport interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.5.0	Command was expanded to include the basic rate interface (BRI).
Release R11.2.0	Command was expanded to include the very high-speed digital subscriber line (VDSL).
Release R11.5.0	Command was expanded to include the EVC option.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example clears all counters associated with the Ethernet 0/1 interface:

>enable
#clear counters ethernet 0/1

clear counters crypto ipsec sa peak

Use the **clear counters crypto ipsec sa peak** command to clear peak Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) security association (SA) count statistics associated with IP security (IPsec).

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example clears the peak IPv4 and IPv6 SA count statistics:

```
>enable
#clear counters crypto ipsec sa peak
```

clear counters dynamic-counter

Use the **clear counters dynamic-counter** command to clear dynamic counter statistics. Variations of the command include:

clear counters dynamic-counter
clear counters dynamic-counter <*slot/index*>

Syntax Description

<*slot/index*>	Optional. Specifies the slot and port of the dynamic counter in the format <*slot/port*>. For example, **0/1**.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example clears all dynamic counter statistics:

>**enable**
#clear counters dynamic-counter

clear counters efm-group *<group number>*

Use the **clear counters efm-group** command to clear the counters of the specified Ethernet in the first mile (EFM) group.

Syntax Description

<group number>	Specifies the EFM group. Range is **1** to **1024**.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example clears the counters for the EFM group **1**:

```
>enable
#clear counters efm-group 1
```

clear counters ethernet cfm

Use the **clear counters ethernet cfm** command to clear all statistics held by Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoints (MEPs). Variations of this command include:

clear counters ethernet cfm
clear counters ethernet cfm domain <*domain name*> **association** <*association name*>
clear counters ethernet cfm domain none association <*association name*>
clear counters ethernet cfm interface <*interface*>
clear counters ethernet cfm level <*level*>
clear counters ethernet cfm mep-id <*mep id*>

Syntax Description

domain <*domain name*>	Optional. Specifies that only statistics for MEPs in the named domain are cleared.
domain none	Optional. Specifies that no domain is named and all MEP statistics, regardless of domain, are cleared.
association <*association name*>	Optional. Specifies that only statistics for MEPs in the named association are cleared.
interface <*interface*>	Optional. Specifies that only statistics for MEPs configured on the specified interface are cleared. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.
level <*level*>	Optional. Specifies that only statistics for MEPs within the specified maintenance domain level are cleared. Level range is **0** to **7**.
mep-id <*mep id*>	Optional. Specifies that only statistics for MEPs with the specified MEP ID are cleared. MEP ID range is **1** to **8191**.

Default Values

No default values necessary for this command.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example clears all statistics associated with Ethernet OAM CFM MEPs:

>**enable**
#clear counters ethernet cfm

The following example clears all statistics associated with MEPs on maintenance domain level **5**:

>**enable**
#clear counters ethernet cfm level 5

clear counters global-policer

Use the **clear counters global-policer** command to clear the virtual AOS (vAOS) global policer statistics. This command clears the global policer dropped packets and dropped bytes counters. The licensed rate drops on each policed interface are also cleared.

Syntax Description

No additional subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R12.1.0	Command was introduced.

Usage Examples

The following example clears the vAOS global policer statistics:

```
>enable
#clear counters global-policer
```

clear counters hmr

Use the **clear counters hmr** command to clear any Session Initiation Protocol (SIP) header manipulation rules (HMR) statistics. Variations of this command include:

clear counters hmr
clear counters hmr direction inbound
clear counters hmr direction outbound
clear counters hmr policy <*name*>
clear counters hmr user <*extension*>
clear counters hmr user global
clear counters hmr user proxy-server
clear counters hmr user proxy-user

Syntax Description

direction inbound	Optional. Clears HMR statistics for inbound SIP traffic.
direction outbound	Optional. Clears HMR statistics for outbound SIP traffic.
policy <*name*>	Optional. Clears HMR statistics for a specific HMR policy.
user	Optional. Clears HMR statistics for a specific user.
<*extension*>	Optional. Clears HMR statistics for a specific user.
global	Optional. Clears HMR statistics for SIP global traffic.
proxy-server	Optional. Clears HMR statistics for SIP proxy server traffic.
proxy-user	Optional. Clears HMR statistics for SIP proxy user traffic.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example clears all HMR statistics:

>enable
#clear counters hmr

clear counters media-gateway

Use the **clear counters media-gateway** command to reset cumulative totals for all Realtime Transport Protocol (RTP) channels or for a specific RTP channel. Variations of this command include the following:

clear counters media-gateway
clear counters media-gateway channel <*value*>
clear counters media-gateway dtmf

Syntax Description

channel <*value*>	Optional. Specifies the ID of a particular media-gateway channel to be reset (for example, **0/1.1**).
dtmf	Optional. Specifies that dual tone multi-frequency (DTMF) counters are reset.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release A2	Command was expanded to include the **dtmf** parameter.

Usage Examples

The following example resets the counters on media gateway **channel 0/1.1**:

>**enable**
#clear counters media-gateway channel 0/1.1
Counters on media-gateway channel reset by console.

clear counters probe

Use the **clear counters probe** command to reset counters on all probe objects or on a specific probe. Variations of this command include:

clear counters probe
clear counters probe <*name*>

Syntax Description

<*name*>	Specifies a probe object to reset counter.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example resets the counters for all configured probes:

>**enable**
#clear counters probe

The following example resets the counters only for the probe named **probe_A**:

>**enable**
#clear counters probe probe_A

clear counters shdsl <*slot/port*> splice-detect

Use the **clear counters shdsl splice-detect** command to clear all bad splice detection test data for the specified single-pair high-speed digital subscriber line (SHDSL) interface.

Syntax Description

<*slot/port*>	Specifies the slot and port of the interface for which you want to clear the test data.

Default Values

No default values are necessary for this command.

Command History

Release A4.05	Command was introduced.

Usage Examples

The following example clears all bad splice detection test data associated with the SHDSL 1/1 interface:

```
>enable
#clear counters shdsl 1/1 splice-detect
```


clear counters track

Use the **clear counters track** command to reset counters on all track objects or on a specifically named track.

clear counters track
clear counters track <*name*>

Syntax Description

<*name*>	Specifies a track object to reset counter.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example resets the counters for all configured tracks:

>**enable**
#clear counters track

The following example resets the counters only for the track named **track_1**:

>**enable**
#clear counters track track_1

clear counters vlan *<vlan id>*

Use the **clear counters vlan** command to reset counters on the specified virtual local area network (VLAN) interface.

Syntax Description

<vlan id>	Specifies a valid VLAN interface ID. Range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example resets the counters on VLAN interface 7:

```
>enable
#clear counters vlan 7
```


clear counters voice-trunk

Use the **clear counters voice-trunk** command to reset counters on all voice trunks or on a specific voice trunk. Variations of this command include:

clear counters voice-trunk all
clear counters voice-trunk <*trunk id*>

Syntax Description

all	Clears all voice trunk counters.
<*trunk id*>	Specifies clearing a specific voice trunk using the trunk's two-digit identifier following T (for example, T01).

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example resets the counters for all configured voice trunks:

>**enable**
#clear counters voice-trunk all

clear crypto ike sa

Use the **clear crypto ike sa** command to clear existing Internet key exchange (IKE) security associations (SAs). Use the **policy** and **remote-id** options to clear specific SAs without clearing them all. Variations of this command include:

clear crypto ike sa
clear crypto ike sa peak
clear crypto ike sa policy <*value*>
clear crypto ike sa remote-id <*remote id*>

Syntax Description

peak	Optional. Clears the peak IKE SA count reached.
policy <*value*>	Optional. Removes all IKE SAs associated with the specified policy priority value. This number is assigned using the command *crypto ike on page 1247*.
remote-id <*remote id*>	Optional. Removes all IKE SAs associated with the specified IKE remote ID. A delete payload is sent to the peers prior to deletion of the SA. This command is preferred to the **clear crypto ike sa policy** <*value*> command when multiple unique SAs have been created on the same IKE policy, but the user wants to delete only the SA to a unique peer.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 12.1	Command was expanded to include the **policy** and **remote-id** parameters.
Release 17.5	Command was expanded to include the **peak** parameter.

Usage Examples

The following example clears the entire database of IKE SAs (including the active associations):

>enable
#clear crypto ike sa

The following example clears IKE SAs associated with **policy 101**:

>enable
#clear crypto ike sa policy 101

The following example clears an IKE SA associated with **remote-id netvanta**:

>enable
#clear crypto ike sa remote-id netvanta

clear crypto ipsec sa

Use the **clear crypto ipsec sa** command to clear existing Internet Protocol security (IPsec) security associations (SAs), including active ones. Variations of this command include the following:

clear crypto ipsec sa
clear crypto ipsec sa entry <*ip address*> **ah** <*SPI*>
clear crypto ipsec sa entry <*ip address*> **esp** <*SPI*>
clear crypto ipsec sa map <*name*>
clear crypto ipsec sa peak
clear crypto ipsec sa peer <*ip address*>
clear crypto ipsec sa remote-id <*remote-id*>

Syntax Description

entry <*ip address*>	Optional. Clears only the SAs related to the specified destination IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
ah <*SPI*>	Optional. Clears only a portion of the SAs by specifying the Authentication Header (AH) Protocol and a security parameter index (SPI). You can determine the correct SPI value using the **show crypto ipsec sa** command.
esp <*SPI*>	Optional. Clears only a portion of the SAs by specifying the Encapsulating Security Payload (ESP) Protocol and an SPI. You can determine the correct SPI value using the **show crypto ipsec sa** command.
map <*name*>	Optional. Clears only the SAs associated with the specified crypto map.
peak	Optional. Clears the peak IPsec SA count reached.
peer <*ip address*>	Optional. Clears only the SAs associated with the specified far-end IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
remote-id <*remote-id*>	Optional. Removes all IPsec SAs associated with the specified IPsec remote ID.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 15.1	Command was expanded to include the **remote-id** parameter.
Release 17.5	Command was expanded to include the **peak** parameter.

Usage Examples

The following example clears all IPsec SAs:

>**enable**
#clear crypto ipsec sa

The following example clears the IPsec SA used for ESP traffic with the SPI of 300 to IP address **63.97.45.57**:

>**enable**
#clear crypto ipsec sa entry 63.97.45.57 esp 300

clear crypto keystore

Use the **clear crypto keystore** command to remove all stored cryptographic key pairs on a device and update the running configuration.

This command cannot be undone. Deleted key pairs cannot be recovered.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

The command prompts you to confirm before deleting the key pairs. You must enter either **yes** or **no** at the prompt. You will also be prompted to specify whether you want to save the system configuration, which will save the running configuration to the unit's nonvolatile random access memory (NVRAM). Even if you do not save the system configuration, the key pairs are still deleted from the device.

Usage Examples

The following example removes all stored cryptographic key pairs and saves the system configuration:

>**enable**
#clear crypto keystore
This will erase all stored key pairs. All self-generated and CA-signed
certificates will be deleted. This action is irreversible. Proceed? [yes/no] **yes**
All stored key pairs have been successfully deleted.
Associated certificates have been removed from the current system
configuration.
Save System Configuration? [y/n] **y**
Building configuration. . .
Done. Success!

clear desktop-auditing

Use the **clear desktop-auditing** command to remove the collected network access protection (NAP) statistics for clients connected to the network. Statistics can be cleared for a single client or for all clients. Variations of this command include:

clear desktop-auditing
clear desktop-auditing host <*hostname*>
clear desktop-auditing interface gigabit-switchport <*slot/port*>
clear desktop-auditing ip <*ip address*>
clear desktop-auditing mac <*mac address*>
clear desktop-auditing vlan <*vlan id*>

Syntax Description

host <*hostname*>	Optional. Clears the statistics for the client with the specified host name.
interface gigabit-switchport <*slot/port*>	Optional. Clears the statistics for the client using the specified interface.
ip <*ip address*>	Optional. Clears the statistics for the client with the specified IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
mac <*mac address*>	Optional. Clears the statistics for the client with the specified medium access control (MAC) address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
vlan <*vlan id*>	Optional. Clears the statistics for the client with the specified virtual local area network (VLAN) identification number. VLAN IDs range from **1** to **4096**.

Default Values

No default values are necessary for this command.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following example clears all collected NAP statistics for all clients:

>**enable**
#clear desktop-auditing

The following example clears all collected NAP statistics for the client with the MAC address **00:A0:C8:00:00:01**:

>**enable**
#clear desktop-auditing mac 00:A0:C8:00:00:01

clear dot11 client *<mac address>*

Use the **clear dot11 client** command to disassociate with the client that has the specified medium access control (MAC) address.

Syntax Description

<mac address>	Specifies the MAC address of the client for which disassociation is desired. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release15.1	Command was introduced.

Usage Examples

The following example disassociates with a client with the MAC address 00:40:96:AB:38:5E:

```
>enable
#clear dot11 client 00:40:96:AB:38:5E

This Station has been removed.
```

clear dump-core

The **clear dump-core** command clears diagnostic information appended to the output of the **show version** command. This information results from an unexpected unit reboot.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example clears the entire database of Internet key exchange (IKE) SAs (including the active associations):

```
>enable
#clear dump-core
```

clear ethernet cfm mep remote

Use the **clear ethernet cfm mep remote** command to clear remote maintenance endpoint (MEP) entries from the Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) continuity check message (CCM) database. Variations of this command include:

clear ethernet cfm mep remote
clear ethernet cfm mep remote domain <*domain name*> **association** <*association name*>
clear ethernet cfm mep remote domain none association <*association name*>
clear ethernet cfm mep remote mep-id <*mep id*>
clear ethernet cfm mep remote remote-mep <*mep id*>

Syntax Description

domain <*domain name*>	Optional. Specifies that only statistics for remote MEPs in the named domain are cleared.
domain none	Optional. Specifies that no domain is named and all remote MEP statistics, regardless of domain, are cleared.
association <*association name*>	Optional. Specifies that only statistics for remote MEPs in the named association are cleared.
mep-id <*mep id*>	Optional. Specifies that only statistics for local MEPs with the specified MEP ID are cleared. MEP ID range is **1** to **8191**.
remote mep-id <*mep id*>	Optional. Specifies that only statistics for remote MEPs with the specified MEP ID are cleared. MEP ID range is **1** to **8191**.

Default Values

No default values are necessary for this command.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example clears all CCM entries for all remote MEPs:

```
>enable
#clear ethernet cfm mep remote
```


clear ethernet lmi statistics

Use the **clear ethernet lmi statistics** command to clear all Ethernet local management interface (E-LMI) statistics, or all E-LMI statistics for a specified interface. Variations of this command include:

clear ethernet lmi statistics
clear ethernet lmi statistics interface <*interface*>

Syntax Description

interface <*interface*>	Optional. Specifies an interface on which to clear E-LMI statistics. Specify interfaces in the format <*interface type [slot/port]*>. For example, for a Gigabit Ethernet interface, use **gigabit eth 0/1**. Type **clear ethernet lmi statistics ?** for a complete list of interfaces.

Default Values

No default values necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example clears all E-LMI statistics on all interfaces:

>enable
#clear ethernet lmi statistics

clear ethernet oam statistics

Use the **clear ethernet oam statistics** command to clear Ethernet Link operations, administration, and management (OAM) statistics on the interface. Ethernet Link OAM statistical information cleared includes Protocol Data Unit (PDU) counters, critical link fault records, and link-monitor events. Variations of this command include:

clear ethernet oam statistics
clear ethernet oam statistics interface <*interface*>

Syntax Description

interface <*interface*>	Optional. Clears the Ethernet Link OAM statistics only on the specified interface. If no interface is specified, then statistics on all interfaces with Ethernet Link OAM enabled are cleared. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id. subinterface id]>*. For example, for a Gigabit Ethernet interface, use **giga-eth 0/1**. For an Ethernet in the first mile (EFM) group, use **efm-group 1/1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example clears all Ethernet Link OAM statistics for the Gigabit Ethernet interface **0/1**:

>enable
#clear ethernet oam statistics interface gigabit-ethernet 0/1

clear ethernet y1731 file-save

Use the **clear ethernet y1731 file-save** command to delete all Y.1731 performance monitoring log files and clears the current historical information stored in RAM.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.6.0	Command was introduced.

Usage Examples

The following example deletes all Y.1731 performance monitoring log files:

(config)**#clear ethernet y1731 file-save**

clear event-history

Use the **clear event-history** command to clear all messages logged to the local event-history.

*Messages cleared from the local event-history (using the **clear event-history** command) are no longer accessible.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example clears all local event-history messages:

```
>enable
#clear event-history
```

clear gvrp statistics

Use the **clear gvrp statistics** command to clear counter statistics on GARP VLAN Registration Protocol (GVRP) interfaces. Variations of this command include:

clear gvrp statistics all
clear gvrp statistics interface <*interface*>

Syntax Description

all	Clears the information for all GVRP interfaces.
interface <*interface*>	Clears the information for the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear gvrp statistics interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example clears counter statistics on the GVRP interfaces:

>**enable**
#clear gvrp statistics all

clear host

Use the **clear host** command to clear a host name when using the domain naming system (DNS) proxy. Variations of this command include:

clear host *
clear host <*hostname*>
clear host vrf <*name*> <*hostname*>

Syntax Description

*	Clears all hosts from the host table.
<*hostname*>	Clears a specific host entry from the host-to-address table.
vrf <*name*>	Optional. Clears the host table entry for a specific virtual routing and forwarding (VRF).

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example clears all dynamic host names:

>**enable**
#clear host *

clear ip access-list

Use the **clear ip access-list** command to clear all counters associated with all Internet Protocol version 4 (IPv4) access control lists (ACLs) or a specified IPv4 ACL. Variations of this command include:

clear ip access-list
clear ip access-list *<ipv4 acl name>*

Syntax Description

<ipv4 acl name>	Optional. Specifies the name (label) of an IPv4 ACL to clear.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Usage Examples

The following example clears all counters for the IPv4 ACL labeled **MatchAll**:

>**enable**
#clear ip access-list MatchAll

clear ip cache

Use the **clear ip cache** command to delete cache table entries. Add the **counters** parameter to reset the counters on the cache table. The command can be limited to a specific virtual routing and forwarding (VRF). Variations of this command include:

clear ip cache
clear ip cache counters
clear ip cache vrf <*name*>
clear ip cache vrf <*name*> **counters**

Syntax Description

counters	Optional. Resets counters in the cache table.
vrf <*name*>	Optional. Clears all fast-cache entries for a specific VRF.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 14.1	Command was expanded to include the **counters** parameter.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example removes all entries from the cache table:

>**enable**
#clear ip cache

The following example resets all fast-cache entries just for the VRF **RED**:

>**enable**
#clear ip cache vrf RED counters

clear ip crypto ipsec sa

Use the **clear ip crypto ipsec sa** command to clear existing Internet Protocol security (IPsec) security associations (SAs), including active ones. Variations of this command include the following:

clear ip crypto ipsec sa
clear ip crypto ipsec sa entry <*ip address*> **ah** <*SPI*>
clear ip crypto ipsec sa entry <*ip address*> **esp** <*SPI*>
clear ip crypto ipsec sa map <*name*>
clear ip crypto ipsec sa peak
clear ip crypto ipsec sa peer <*ip address*>
clear ip crypto ipsec sa profile <*name*>
clear ip crypto ipsec sa remote-id <*remote-id*>

Syntax Description

entry <*ip address*>	Optional. Clears only the SAs related to the specified destination IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
ah <*SPI*>	Optional. Clears only a portion of the SAs by specifying the Authentication Header (AH) Protocol and a security parameter index (SPI). You can determine the correct SPI value using the **show crypto ipsec sa** command.
esp <*SPI*>	Optional. Clears only a portion of the SAs by specifying the Encapsulating Security Payload (ESP) Protocol and an SPI. You can determine the correct SPI value using the **show crypto ipsec sa** command.
map <*name*>	Optional. Clears only the SAs associated with the specified crypto map.
peak	Optional. Clears the peak IPsec SA count reached.
peer <*ip address*>	Optional. Clears only the SAs associated with the specified far-end IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
profile <*name*>	Optional. Clears only the SAs created in association with the specified IPsec profile name.
remote-id <*remote-id*>	Optional. Removes all IPsec SAs associated with the specified IPsec remote ID.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 15.1	Command was expanded to include the **remote-id** parameter.
Release 17.5	Command was expanded to include the **peak** parameter.
Release R10.5.0	Command syntax was changed to require the **ip** keyword.
Release R11.9.0	Command was expanded to include the **profile** <*name*> parameter.

Usage Examples

The following example clears all IPsec SAs:

>**enable**
#clear ip crypto ipsec sa

The following example clears the IPsec SA used for ESP traffic with the SPI of **300** to IP address **63.97.45.57**:

>**enable**
#clear ip crypto ipsec sa entry 63.97.45.57 esp 300

clear ip dhcp binding

Use the **clear ip dhcp binding** command to clear Dynamic Host Configuration Protocol version 4 (DHCPv4) server binding entries. Variations of this command include:

clear ip dhcp binding *
clear ip dhcp binding <*ipv4 address*>
clear ip dhcp binding vrf <*name*> *
clear ip dhcp binding vrf <*name*> <*ipv4 address*>

Syntax Description

*****	Clears all automatic DHCPv4 server binding entries.
vrf <*name*>	Optional. Clears DHCPv4 server binding entries on the specified virtual routing and forwarding (VRF) instance.
<*ipv4 address*>	Clears a specific DHCPv4 server binding associated with an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command syntax was changed to remove the hyphen and the **server** keyword for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **server** keyword for Adtran voice products.

Usage Examples

The following example clears all DHCPv4 server bindings on the default VRF:

```
>enable
#clear ip dhcp binding *
```

The following example clears all DHCPv4 server bindings from the VRF RED:

```
>enable
#clear ip dhcp binding vrf RED *
```

clear ip ffe

Use the **clear ip ffe** command to remove the RapidRoute Engine entries on all interfaces or on a specific interface. Variations of this command include:

clear ip ffe
clear ip ffe *<interface>*
clear ip ffe *<interface>* **peak**
clear ip ffe ipsec
clear ip ffe ipsec *<rapidroute interface ID>*
clear ip ffe ipsec *<rapidroute interface ID>* **peak**
clear ip ffe ipsec peak
clear ip ffe peak
clear ip ffe system-control-evc
clear ip ffe system-control-evc peak
clear ip ffe system-management-evc
clear ip ffe system-management-evc peak

Syntax Description

<interface>	Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**. Type **clear ip ffe?** for a complete list of valid interfaces.
ipsec	Specifies that all RapidRoute entries to and from an Internet Protocol security (IPsec) security association (SA) are cleared.
<rapidroute interface ID>	Specifies that RapidRoute entries to and from an IPsec SA on a specified RapidRoute interface are cleared. RapidRoute interface identifiers range from **1** to **16777215**.
peak	Clears the RapidRoute peak entry count. If no interface is specified, the peak entry counts for all interfaces are cleared.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include **ipsec** parameters.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Release R.10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R11.3.0	Command was expanded to include the Ethernet in the first mile (EFM) group and Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.10.0	Command was expanded to include the **peak** parameter.

Usage Examples

The following example clears all RapidRoute entries for the Ethernet 0/1 interface:

>**enable**
#clear ip ffe ethernet 0/1

The following example clears the RapidRoute peak entry count for all interfaces:

>**enable**
#clear ip ffe peak

clear ip flow stats

Use the **clear ip flow stats** command to clear all statistics associated with an integrated traffic monitoring (ITM) observation point.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example clears all ITM statistics associated with an observation point:

#clear ip flow stats

clear ip flow top-talkers

Use the **clear ip flow top-talkers** command to clear all statistics associated with integrated traffic monitoring (ITM) Top Talker listings.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example clears all Top Talker statistics:

#clear ip flow top-talkers

clear ip igmp group

Use the **clear ip igmp group** command to clear entries from the Internet Group Management Protocol (IGMP) tables. If no address or interface is specified, all nonstatic IGMP groups are cleared with this command. Variations of this command include:

clear ip igmp group
clear ip igmp group <*multicast address*>
clear ip igmp group <*interface*>

Syntax Description

<*multicast address*>	Optional. Clears the IGMP tables of a specific multicast group IP address. The multicast group IP address range is **244.0.0.0** to **239.255.255.255** or **224.0.0.0 /4**.
<*interface*>	Optional. Clears the IGMP tables of all interfaces of the specified type or a specific interface of a particular type. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear ip igmp group ?** for a list of valid interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include the high-bit-rate digital subscriber line (HDSL) and tunnel interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Usage Examples

The following example clears all statistics from the IGMP tables for all nonstatic IGMP groups:

>**enable**
#clear ip igmp group

clear ip nhrp

Use the **clear ip nhrp** command to clear all Next Hop Resolution Protocol (NHRP) cache entries. Variations of this command include:

clear ip nhrp
clear ip nhrp <*destination ipv4 address*>
clear ip nhrp <*number*>

Syntax Description

<*destination ipv4 address*>	Optional. Specifies that only cache entries matching this address are cleared. Express IPv4 addresses in dotted decimal notation; for example, **10.10.10.1**.
<*number*>	Optional. Specifies that only cache entries matching the Generic Routing Encapsulation (GRE) multipoint tunnel interface number are cleared. Valid range is **1** to **1024**.

Default Values

No default values are necessary for this command.

Command History

Release R11.9.0	Command was introduced.

Usage Examples

The following example clears all NHRP cache entries:

>**enable**
#clear ip nhrp

clear ip ospf

Use the **clear ip ospf** command to reset Open Shortest Path First version 2 (OSPFv2) information. Variations of this command include:

clear ip ospf process
clear ip ospf redistribution

Syntax Description

process	Restarts the OSPF process.
redistribution	Refreshes routes redistributed over OSPF.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example resets the OSPF process:

```
>enable
#clear ip ospf process
```


clear ip policy-sessions

Use the **clear ip policy-sessions** command to clear Internet Protocol version 4 (IPv4) access control policy (ACP) firewall sessions. You may clear all the IPv4 sessions or a specific session. Use the **show ip policy-sessions** command to view a current IPv4 session listing. Variations of this command include:

clear ip policy-sessions
clear ip policy-sessions any-vrf
clear ip policy-sessions pending
clear ip policy-sessions *<ipv4 acp name>* **[ahp | esp | gre | icmp | tcp | udp |** *<protocol>***]** *<ipv4 source> <source port> <ipv4 destination> <destination port>*
clear ip policy-sessions *<ipv4 acp name>* **[ahp | esp | gre | icmp | tcp | udp |** *<protocol>***]** *<ipv4 source> <source port> <ipv4 destination> <destination port>* **[destination | source]** *<nat ipv4 address> <nat address port>*
clear ip policy-sessions vrf *<name>*
clear ip policy-sessions vrf *<name> <ipv4 acp name>* **[ahp | esp | gre | icmp | tcp | udp |** *<protocol>***]** *<ipv4 source> <source port> <ipv4 destination> <destination port>*
clear ip policy-sessions vrf *<name> <ipv4 acp name>* **[ahp | esp | gre | icmp | tcp | udp |** *<protocol>***]** *<ipv4 source> <source port> <ipv4 destination> <destination port>* **[destination | source]** *<nat ipv4 address> <nat port>*

Syntax Description

any-vrf	Optional. Clears the current ACP associations for all virtual routing and forwarding (VRF) instances.
pending	Optional. Clears pending ACP associations that are waiting on unknown traffic.
<ipv4 acp name>	Optional. Specifies the IPv4 ACP from which to clear the firewall sessions.
ahp	Specifies Authentication Header (AH) Protocol.
esp	Specifies Encapsulating Security Payload (ESP) Protocol.
gre	Specifies Generic Routing Encapsulation (GRE) Protocol.
icmp	Specifies Internet Control Message Protocol (ICMP).
tcp	Specifies Transmission Control Protocol (TCP).
udp	Specifies User Datagram Protocol (UDP).
<protocol>	Specifies a protocol. Valid range is **0** to **255**.
<ipv4 source>	Optional. Specifies the source IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<source port>	Optional. Specifies the source port (in hex format AH, ESP, and GRE; decimal for all other protocols).
<ipv4 destination>	Optional. Specifies the destination IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<destination port>	Optional. Specifies the destination port (in hex format for AH, ESP, and GRE; decimal for all other protocols).
[destination | source]	Optional. For network address translation (NAT) sessions, this specifies whether to select a NAT source or NAT destination session.

<nat ipv4 address>	Optional. For NAT sessions, this specifies the NAT IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<nat port>	Optional. For NAT sessions, this specifies the NAT port (in hex format for AH, ESP, and GRE; decimal for all other protocols).
vrf *<name>*	Optional. Specifies the VRF instance to impact. Executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Clearing pending ACP sessions may temporarily disrupt any applications that depend on the presence of pending ACP sessions to allow the application traffic through the firewall.

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.
Release 17.1	Command was expanded to include the **vrf** and **any-vrf** parameters.
Release R10.1.0	Command was expanded to include the **pending** parameter.

Functional Notes

The second half of this command, beginning with the source IPv4 address, may be copied and pasted from a row in the **show ip policy-sessions** table for easier use.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example clears the Telnet association (TCP port **23**) for an IPv4 policy class **PCLASS1** with source IPv4 address **192.22.71.50** and destination **192.22.71.130**:

```
>enable
#clear ip policy-sessions PCLASS1 tcp 192.22.71.50 23 192.22.71.130 23
```

The following example clears all IPv4 policy class sessions for the VRF instance named **RED**:

```
>enable
#clear ip policy-sessions vrf RED
```


clear ip policy-stats

Use the **clear ip policy-stats** command to clear statistical counters for Internet Protocol version 4 (IPv4) access control policies (ACPs). Variations of this command include:

clear ip policy-stats
clear ip policy-stats <*ipv4 acp name*>
clear ip policy-stats <*ipv4 acp name*> **entry** <*number*>

Syntax Description

<*ipv4 acp name*>	Optional. Specifies the IPv4 ACP to clear. If no IPv4 ACP is specified, statistics are cleared for all policies.
entry <*number*>	Optional. Clears the statistics of a specific IPv4 ACP. Number range is **1** to **4294967295**.

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example clears statistical counters for all IPv4 ACPs:

>**enable**
#clear ip policy-stats

The following example clears statistical counters for the IPv4 ACP **MatchALL**:

>**enable**
#clear ip policy-stats MatchALL

clear ip prefix-list *<name>*

Use the **clear ip prefix-list** command to clear the IP prefix list hit count shown in the **show ip prefix-list detail** command output. Refer to *show ip prefix-list on page 771* for more information.

Syntax Description

<name>	Clears the count statistics of the specified IP prefix list.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example clears the hit count statistics for prefix list **test**:

```
>enable
#clear ip prefix-list test
```


clear ip route

Use the **clear ip route** command to remove all learned routes from the IP route table. Static and connected routes are not cleared by this command. The command can be limited to a specific virtual routing and forwarding (VRF). Variations of this command include:

clear ip route *
clear ip route <*ip address*> <*subnet mask*>
clear ip route vrf <*name*> ***
clear ip route vrf <*name*> <*ip address*> <*subnet mask*>

Syntax Description

*****	Deletes all destination routes.
<*ip address*>	Specifies the IP address of the destination routes to be deleted. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IP addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
vrf <*name*>	Optional. Clears the IP route table for the specified VRF.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example removes all learned routes from the route table:

>**enable**
#clear ip route *

The following example removes all learned routes from the route table on the VRF **RED**:

>**enable**
#clear ip route vrf RED *

clear ip route-cache express

Use the **clear ip route-cache express** command to remove all routes from the hardware forwarding table.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example clears all routes from the hardware forwarding table:

```
>enable
#clear ip route-cache express
```

clear ip security

Use the **clear ip security** command to clear all statistics associated with the security monitor. Variations of this command include:

clear ip security any-vrf threats
clear ip security monitor
clear ip security threats
clear ip security vrf <*name*> **threats**

Syntax Description

any-vrf threats	Clears statistics on any available VRF on the device.
monitor	Clears all statistics associated with the security monitor.
threats	Clears the IP security threats list.
vrf <*name*> **threats**	Clears statistics on the named VRF.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Functional Notes

The **clear ip security** command is used to clear all statistics associated with the security monitor including policy-stats and excluding timeline and virtual private network (VPN) statistics. The time of the clear is saved.

Usage Examples

The following example clears threat statistics for the named VRF **MyVRF**:

>**enable**
#clear ip security vrf MyVRF threats

clear ip urlfilter statistics

Use the **clear ip urlfilter statistics** command to clear all statistics counters for uniform resource locator (URL) filter requests and responses.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example clears all counters for URL filter requests and responses:

```
>enable
#clear ip urlfilter statistics
```

clear ip urlfilter top-websites

Use the **clear ip urlfilter top-websites** command to clear all statistics for top websites reporting.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example clears all statistics for top websites reporting:

```
>enable
#clear ip urlfilter top-websites
```


clear ipv6 access-list

Use the **clear ip access-list** command to clear all counters associated with all Internet Protocol version 6 (IPv6) access control lists (ACLs) or a specified IPv6 ACL. Variations of this command include:

clear ipv6 access-list
clear ipv6 access-list <*ipv6 acl name*>

Syntax Description

<*ipv6 acl name*>	Optional. Specifies the name (label) of an IPv6 ACL to clear.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example clears all counters for the IPv6 ACL labeled **MatchAll**:

>**enable**
#clear ipv6 access-list MatchAll

clear ipv6 cache

Use the **clear ipv6 cache** command to clear all the Internet Protocol version 6 (IPv6) route cache entries in a given virtual routing and forwarding (VRF) instance. Variations of this command include:

clear ipv6 cache
clear ipv6 cache counters
clear ipv6 cache vrf <*name*>
clear ipv6 cache vrf <*name*> **counters**

Syntax Description

counters	Optional. Specifies that only the use-count statistics are cleared for each IPv6 route cache entry.
vrf <*name*>	Optional. Specifies a nondefault VRF instance on which to clear all the IPv6 route cache entries. If no VRF instance is specified, all entries on the default VRF instance are cleared.

Default Values

No default values are necessary for this command.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example clears all the IPv6 route cache entries on the default VRF instance:

>**enable**
#clear ipv6 cache

clear ipv6 dhcp binding

Use the **clear ipv6 dhcp binding** command to remove one or all of the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) server binding entries. Variations of this command include:

clear ipv6 dhcp binding *
clear ipv6 dhcp binding <*ipv6 address*>
clear ipv6 dhcp binding client-identifier <*client DUID*>
clear ipv6 dhcp binding vrf <*name*> *
clear ipv6 dhcp binding vrf <*name*> <*ipv6 address*>
clear ipv6 dhcp binding vrf <*name*> **client-identifier** <*client DUID*>

Syntax Description

*****	Clears all DHCPv6 server IPv6 address bindings.
<*ipv6 address*>	Clears DHCPv6 server bindings for a single IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
client-identifier <*client DUID*>	Clears the DHCPv6 server bindings for a single DHCPv6 client. The client DHCP unique identifier (DUID) is expressed as a hexadecimal value.
vrf <*name*>	Optional. specifies a nondefault virtual routing and forwarding (VRF) instance from which to remove the binding entries. If no VRF instance is specified, the binding entries are cleared on the default VRF instance.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example specifies that the DHCPv6 server bindings on the default VRF instance for all IPv6 addresses are cleared:

>enable
#clear ipv6 dhcp binding *

clear ipv6 dhcp client <*interface*>

Use the **clear ipv6 dhcp client** command to reinitialize the entire Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the specified interface. Using this command releases and renews ALL parameters requested or assigned using DHCPv6 to this client. This includes addresses, prefixes, and any other configuration information. Variations of this command include:

clear ipv6 dhcp client <*interface*>
clear ipv6 dhcp client mef-ethernet <*slot/port*>
clear ipv6 dhcp client system-control-evc
clear ipv6 dhcp client system-management-evc

Syntax Description

<*interface*>	Specifies the client interface on which to reinitialize the DHCPv6 information. Specify interfaces in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**. Type **clear ipv6 dhcp client ?** for a complete list of valid interfaces.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.

Default Values

No default values are necessary for this command.

Command History

Release R10.9.0	Command was introduced.
Release R.10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Usage Examples

The following example reinitializes the entire client and all its associated information for the Ethernet 0/1 interface:

>**enable**
#clear ipv6 dhcp client ethernet 0/1

clear ipv6 dhcp conflict

Use the **clear ipv6 dhcp conflict** command to remove one or all of the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) server addresses that conflict. Variations of this command include:

clear ipv6 dhcp conflict *
clear ipv6 dhcp conflict <*ipv6 address*>
clear ipv6 dhcp conflict vrf <*name*> ***
clear ipv6 dhcp conflict vrf <*name*> <*ipv6 address*>

Syntax Description

*****	Specifies that all IPv6 address conflicts are cleared.
<*ipv6 address*>	Specifies that the conflicts for a single IPv6 address are cleared. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance from which to remove the conflicting address entries. If no VRF instance is specified, the conflicting entries are cleared on the default VRF instance.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example clears the DHCPv6 server conflict addresses on the default VRF instance for all IPv6 addresses:

>**enable**
#clear ipv6 dhcp conflict *

clear ipv6 ffe

Use the **clear ipv6 ffe** command to manually clear Internet Protocol version 6 (IPv6) RapidRoute entries in the fast forwarding engine (FFE) table. Variations of this command include:

clear ipv6 ffe
clear ipv6 ffe peak
clear ipv6 ffe *<interface>*
clear ipv6 ffe *<interface>* **peak**
clear ipv6 ffe system-control-evc
clear ipv6 ffe system-control-evc peak
clear ipv6 ffe system-management-evc
clear ipv6 ffe system-management-evc peak

Syntax Description

<interface>	Optional. Specifies an ingress interface on which to clear all IPv6 RapidRoute entries. If no interface is specified, then all IPv6 RapidRoute entries in the AOS device are cleared. Specify interfaces in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**. Type **clear ip ffe?** for a complete list of valid interfaces.
peak	Clears the RapidRoute peak entry count. If no interface is specified, the peak entry counts for all interfaces are cleared.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.

Default Values

No default values necessary for this command.

Command History

Release R10.4.0	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R.10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R11.10.0	Command was expanded to include the **peak** parameter.

Usage Examples

The following example clears all IPv6 RapidRoute entries on the AOS device:

>**enable**
#clear ipv6 ffe

The following example clears the RapidRoute peak entry count for all interfaces:

>**enable**
#clear ipv6 ffe peak

clear ipv6 interfaces prefix

Use the **clear ipv6 interfaces prefix** command to clear Internet Protocol version 6 (IPv6) address prefix information from a specified interface. Variations of this command include:

clear ipv6 interfaces <*interface*> **prefix**
clear ipv6 mef-ethernet <*slot/port*> **prefix**
clear ipv6 interfaces system-control-evc prefix
clear ipv6 interfaces system-management-evc prefix

Syntax Description

<*interface*>	Specifies the interface on which to clear IPv6 address prefix information. Specify interfaces in the <*interface*> <*slot/port* | *interface id*> format. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. Enter **clear ipv6 interfaces ?** for a list of available interfaces.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R.10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Usage Examples

The following example specifies that all IPv6 address prefix information is cleared for the **ethernet 0/1** interface:

>**enable**
#clear ipv6 interfaces ethernet 0/1 prefix

clear ipv6 mld traffic

Use the **clear ipv6 mld traffic** command to reset Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) traffic counters to zero. Variations of this command include:

clear ipv6 mld traffic
clear ipv6 mld traffic vrf <*name*>

Syntax Description

vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to reset the MLD counters. If no VRF is specified, the counters on the default VRF are reset.

Default Values

No default values are necessary for this command.

Command History

Release R11.4.0	Command was introduced.

Usage Examples

The following example clears the MLD traffic counters on the default VRF:

```
>enable
#clear ipv6 mld traffic
```

clear ipv6 neighbors

Use the **clear ipv6 neighbors** command to clear dynamic entries from the Internet Protocol version 6 (IPv6) neighbor cache. Variations of this command include:

clear ipv6 neighbors <*interface*>
clear ipv6 neighbors <*interface*> <*ipv6 address*>
clear ipv6 neighbors <*interface*> **statistics**
clear ipv6 neighbors [mef-ethernet <*slot/port*> **| system-control-evc** | **system-management-evc]**
clear ipv6 neighbors [mef-ethernet <*slot/port*> **| system-control-evc** | **system-management-evc]** <*ipv6 address*>
clear ipv6 neighbors [mef-ethernet <*slot/port*> **| system-control-evc** | **system-management-evc]** **statistics**
clear ipv6 neighbors vrf <*name*>
clear ipv6 neighbors vrf <*name*> <*ipv6 address*>
clear ipv6 neighbors vrf <*name*> **statistics**

Syntax Description

<*ipv6 address*>	Optional. Specifies that the neighbor cache entries for a specific IPv6 address are cleared. Specify IPv6 addresses in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. If no IPv6 address is specified, all entries are cleared.
<*interface*>	Optional. Specifies that the neighbor cache entries for a specific interface are cleared. Specify interfaces in the <*interface*> <*slot/port* | *interface id*> format. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. If no interface is specified, all entries for all interfaces on the virtual routing and forwarding (VRF) instance are cleared.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
statistics	Optional. Specifies that statistics for the neighbor cache and protocol interaction are cleared.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.
vrf <*name*>	Optional. Specifies that neighbor cache entries for a specific VRF instance are cleared. If no VRF is specified, entries on the default unnamed VRF are cleared.

Default Values

By default, if no options are specified, entering this command clears all neighbor cache entries on all interfaces assigned to the default VRF.

Command History

Release 18.1	Command was introduced.

Release R.10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Usage Examples

The following example clears all entries in the neighbor cache for the default VRF:

>**enable**
#clear ipv6 neighbors

clear ipv6 policy-sessions

Use the **clear ipv6 policy-sessions** command to clear Internet Protocol version 6 (IPv6) access control policy (ACP) sessions from the firewall association database. Clearing a session typically terminates the session's communication, therefore this command should be used carefully, particularly if the session is one used for access to the command line interface (CLI). You may clear all the IPv6 sessions or a specific IPv6 session. Use the **show ipv6 policy-sessions** command to view a current IPv6 session listing. Variations of this command include:

clear ipv6 policy-sessions
clear ipv6 policy-sessions <*ipv6 acp name*> **[ahp | esp | gre |** <*protocol*>**]** <*ipv6 source*> **[**<*interface*>**]** <*ipv6 destination*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions <*ipv6 acp name*> **[tcp | udp]** <*ipv6 source*> **[**<*interface*>**]** <*source port*> <*ipv6 destination*> <*destination port*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions <*ipv6 acp name*> **icmpv6** <*ipv6 source*> **[**<*interface*>**]** <*id*> <*ipv6 destination*> <*type/code*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions any-vrf
clear ipv6 policy-sessions pending
clear ipv6 policy-sessions pending any-vrf
clear ipv6 policy-sessions pending <*ipv6 acp name*> **[ahp | esp | gre |** <*protocol*>**]** <*ipv6 source*> **[**<*interface*>**]** <*ipv6 destination*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions pending <*ipv6 acp name*> **[tcp | udp]** <*ipv6 source*> **[**<*interface*>**]** <*source port* | **unknown**> <*ipv6 destination*> <*destination port* | **unknown**> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions pending <*ipv6 acp name*> **icmpv6** <*ipv6 source*> **[**<*interface*>**]** <*id*> <*ipv6 destination*> <*type/code*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions pending vrf <*name*> <*ipv6 acp name*> **[tcp | udp]** <*ipv6 source*> **[**<*interface*>**]** <*source port* | **unknown**> <*ipv6 destination*> <*destination port* | **unknown**> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions vrf <*name*>
clear ipv6 policy-sessions vrf <*name*> <*ipv6 acp name*> **[ahp | esp | gre |** <*protocol*>**]** <*ipv6 source*> **[**<*interface*>**]** <*ipv6 destination*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions vrf <*name*> <*ipv6 acp name*> **[tcp | udp |** <*protocol*>**]** <*ipv6 source*> **[**<*interface*>**]** <*source port* | **unknown**> <*ipv6 destination*> <*destination port* | **unknown**> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
clear ipv6 policy-sessions vrf <*name*> <*ipv6 acp name*> **icmpv6** <*ipv6 source*> **[**<*interface*>**]** <*id*> <*ipv6 destination*> <*type/code*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**

Syntax Description

any-vrf	Optional. Specifies that all sessions in all virtual routing and forwarding (VRF) instances are cleared.

pending	Optional. Specifies that any associations waiting on unknown traffic are cleared.
<ipv6 acp name>	Optional. Specifies the IPv6 ACP from which to clear the firewall sessions.
ahp	Specifies Authentication Header (AH) Protocol.
esp	Specifies Encapsulating Security Payload (ESP) Protocol.
gre	Specifies Generic Routing Encapsulation (GRE) Protocol.
icmpv6	Specifies Internet Control Message Protocol (ICMP) version 6 (ICMPv6).
mef-ethernet *<slot/port>*	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.
tcp	Specifies Transmission Control Protocol (TCP).
udp	Specifies User Datagram Protocol (UDP).
<protocol>	Specifies a protocol. Valid range is **0** to **255**.
<ipv6 source>	Specifies the source IPv6 address. IPv6 addresses should be expressed in colon hexadecimal notation (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<source port>	Specifies the source port for TCP and UDP sessions. Range is **0** to **65535**.
<ipv6 destination>	Specifies the destination IPv6 address. IPv6 addresses should be expressed in colon hexadecimal notation (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<destination port>	Specifies the destination port for TCP and UDP sessions. Range is **0** to **65535**.
<interface>	Specifies the interface when a link-local IPv6 address is entered (addresses beginning with **FE80::**). Interfaces must be entered when using a link-local address. Specify interfaces in the *<interface> <slot/port* | *interface id>* format. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**.
<id>	Specifies the ICMPv6 ID. Valid range is **0** to **65535**.
<type/code>	Specifies the type and code of the ICMPv6 session to be cleared. Type and code ranges are **0** to **255**.
unknown	Specifies that the source or destination port is unknown.
vrf *<name>*	Optional. Specifies the VRF instance to impact. Executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Release R10.1.0	Command was expanded to include the tunnel interface and the **pending** parameter.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.7.0	Command was expanded to include the **unknown** parameter.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R13.7.0	Command was expanded to include the Gigabit Ethernet and virtual local area network (VLAN) interfaces.

Functional Notes

The second half of this command, beginning with the source IPv6 address, can be copied and pasted from a row in the **show ipv6 policy-sessions** table for easier use.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example clears the Telnet association (TCP port **23**) for IPv6 ACP **pclass1** with source IPv6 address **FE80::2AO:C8FF:FE61:3082** and destination IPv6 address **2003::2AO:C8FF:FE61:3084**. Because the source IPv6 address is a link-local address (**FE80::**), the appropriate interface (in this case **ethernet 0/1**) must be entered after the source IPv6 address. Enter the command as follows:

>**enable**
#clear ipv6 policy-sessions pclass1 tcp FE80::2AO:C8FF:FE61:3082 ethernet 0/1
2003::2AO:C8FF:FE61:3084

The following example clears all IPv6 policy class sessions for the VRF instance named RED:
>**enable**

#clear ipv6 policy-sessions vrf RED

clear ipv6 policy-stats

Use the **clear ipv6 policy-stats** command to clear statistical counters for IPv6 access control policies (ACPs). Variations of this command include:

clear ipv6 policy-stats
clear ipv6 policy-stats <*ipv6 acp name*>
clear ipv6 policy-stats <*ipv6 acp name*> **entry** <*number*>

Syntax Description

<*ipv6 acp name*>	Optional. Specifies the IPv6 ACP statistics to clear. If no IPv6 ACP is specified, statistics are cleared for all IPv6 ACPs.
entry <*number*>	Optional. Specifies only a specific entry within the IPv6 ACP is cleared. Number range is **1** to **4294967295**.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example clears statistical counters for all IPv6 ACPs:

>**enable**
#clear ipv6 policy-stats

The following example clears statistical counters for the IPv6 ACP **MatchALL**:

>**enable**
#clear ipv6 policy-stats MatchALL

The following example clears statistical counters for the **6**th entry in the IPv6 ACP **MatchALL**:

>**enable**
#clear ipv6 policy-stats MatchALL entry 6

clear ipv6 prefix-list *<name>*

Use the **clear ipv6 prefix-list** command to clear statistics associated with the Internet Protocol version 6 (IPv6) prefix list.

Syntax Description

<name>	Clears the hit count statistics of the specified IPv6 prefix list.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example clears the hit count statistics for the IPv6 prefix list **TEST1**:

```
>enable
#clear ipv6 prefix-list TEST1
```


clear ipv6 routers

Use the **clear ipv6 routers** command to clear the Internet Protocol version 6 (IPv6) list of routers learned from router advertisement (RA) messages from locally reachable routers. Variations of this command include:

clear ipv6 routers <*interface*>
clear ipv6 routers <*interface*> **conflict**
clear ipv6 routers [system-control-evc | **system-management-evc]**
clear ipv6 routers [system-control-evc | **system-management-evc] conflict**
clear ipv6 routers vrf <*name*>
clear ipv6 routers vrf <*name*> **conflict**

Syntax Description

<*interface*>	Optional. Specifies an interface from which to clear the learned router list. If no interface is specified, learned routers on all interfaces of the virtual routing and forwarding (VRF) are cleared. Specify interfaces in the <*interface*> <*slot/port* | *interface id*> format. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. Enter **clear ipv6 routers ?** for a list of available interfaces.
conflict	Optional. Specifies that learned routers with misconfigurations are cleared from locally reachable routers.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Specifies the system management EVC. This EVC is preconfigured on the unit.
vrf <*name*>	Optional. Specifies a VRF on which to clear learned routers. If no VRF is specified, learned routers for all interfaces on the default VRF are cleared.

Default Values

By default, all learned routers from all interfaces on the default VRF are cleared when no options are specified.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R.10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.

Usage Examples

The following example specifies that learned routers are cleared from all interfaces on the default VRF:

>enable
#clear ipv6 routers

clear lldp counters interface *<interface>*

Use the **clear lldp counters interface** command to reset all Link Layer Discovery Protocol (LLDP) packet counters to zero on all interfaces.

Syntax Description

<interface>	Clears the information for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear lldp counters interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet and gigabit switchport interfaces.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example resets all LLDP counters:

```
>enable
#clear lldp counters interface
```


clear lldp neighbors

Use the **clear lldp neighbors** command to remove all neighbors from this unit's database. As new Link Layer Discovery Protocol (LLDP) frames are received, the database will contain information about neighbors included in those frames.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command generates output indicating the names of any neighbors deleted from the database and the name of the interface on which the neighbor was learned.

Usage Examples

The following example clears LLDP neighbor **Switch_1** from the Ethernet interface 0/7:

```
>enable
#clear lldp neighbors
LLDP: Deleted neighbor “Switch_1” on interface eth 0/7
#
```

clear mac address-table

Use the **clear mac address-table** command to remove medium access control (MAC) addresses from the MAC address table. Variations of this command include:

clear mac address-table
clear mac address-table <*interface*>

Syntax Description

<*interface*>	Optional. Removes the MAC address of the specified interface. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear mac address-table interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example removes the MAC address of a Gigabit Ethernet interface from the MAC address table:

>**enable**
#clear mac address-table gigabit-ethernet 0/1

clear mac address-table dynamic

Use the **clear mac address-table dynamic** command to remove dynamic medium access control (MAC) addresses from the MAC address table. Variations of this command include:

clear mac address-table dynamic <*interface*>
clear mac address-table dynamic address <*mac address*>

Syntax Description

<*interface*>	Removes the MAC address of the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear mac address-table dynamic interface ?** for a complete list of applicable interfaces.
address <*mac address*>	Removes a specific MAC address from the table. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example removes the dynamic address **A0:B1:C2:D3:E4:A1** from the MAC address table:

```
>enable
#clear mac address-table dynamic address A0:B1:C2:D3:E4:A1
```

The following example removes all dynamic addresses from the MAC address table:

```
>enable
#clear mac address-table dynamic
```

clear mac address-table multicast

Use the **clear mac address-table multicast** command to clear all entries in the multicast address resolution lookup (ARL) table or filter the entries based on certain criteria. Variations of this command include:

clear mac address-table multicast
clear mac address-table multicast igmp-snooping
clear mac address-table multicast user
clear mac address-table multicast vlan <*vlan id*>
clear mac address-table multicast vlan <*vlan id*> **igmp-snooping**
clear mac address-table multicast vlan <*vlan id*> **user**

Syntax Description

igmp-snooping	Optional. Clears entries in the multicast ARL table that were added dynamically (via IGMP snooping).
user	Optional. Clears entries in the multicast ARL table that were added statically (by the user).
vlan <*vlan id*>	Optional. Clears entries in the multicast ARL table based on virtual local area network (VLAN).

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example removes the entries in the multicast ARL table for **VLAN 200**:

>**enable**
#clear mac address-table multicast vlan 200

clear mail-client body *<agent name>*

Use the **clear mail-client body** command to clear the body text of the pending email message for a specific mail agent.

Syntax Description

<agent name>	Specifies which mail agent body text is cleared.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example clears pending email body text for mail agent **myagent**:

```
>enable
#clear mail-client body myagent
```

clear mail-client counters

Use the **clear mail-client counters** command to clear all statistical counters associated with all mail agents. Variations of this command include:

clear mail-client counters
clear mail-client counters *<agent name>*

Syntax Description

<agent name>	Optional. Specifies that only a specific mail agent's counters are cleared.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example clears all counters for all configured mail agents:

>**enable**
#clear mail-client counters

clear network-forensics ip dhcp

Use the **clear network-forensics ip dhcp** command to remove the Dynamic Host Configuration Protocol (DHCP) statistics for clients connected to the network. Statistics can be cleared for a single client or for all clients. Variations of this command include:

clear network-forensics ip dhcp
clear network-forensics ip dhcp hostname <*hostname*>
clear network-forensics ip dhcp interface gigabit-switchport <*slot/port*>
clear network-forensics ip dhcp ip <*ip address*>
clear network-forensics ip dhcp mac <*mac address*>
clear network-forensics ip dhcp vlan <*vlan id*>

Syntax Description

hostname <*hostname*>	Optional. Clears statistics for the client with the specified host name.
interface gigabit-switchport <*slot/port*>	Optional. Clears statistics for the client using the specified interface.
ip <*ip address*>	Optional. Clears the statistics for the client with the specified IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
mac <*mac address*>	Optional. Clears the statistics for the client with the specified medium access control (MAC) address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
vlan <*vlan id*>	Optional. Clears the statistics for the client with the specified virtual local area network (VLAN) identification number. VLAN IDs range from **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following example clears all collected DHCP statistics for all clients:

>**enable**
#clear network-forensics ip dhcp

The following example clears all collected DHCP statistics for the client with the MAC address **00:A0:C8:00:00:01**:

>**enable**
#clear network-forensics ip dhcp mac 00:A0:C8:00:00:01

clear network-sync

Use the **clear network-sync** command to clear network synchronization (Network Sync) related information from the unit's configuration. Variations of this command include:

clear network-sync
clear network-sync info

Syntax Description

info	Optional. Specifies that all Network Sync statistical information is cleared.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example clears all statistical information for Network Sync:

>**enable**
#clear network-sync info

clear ntp

Use the **clear ntp** command to restart the Network Time Protocol (NTP) daemon.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example restarts the NTP daemon:

```
>enable
#clear ntp
```


clear ospfv3

Use the **clear ospfv3** command to reset and restart specific Open Shortest Path First version 3 (OSPFv3) processes, and to refresh routes distributed into OSPFv3 processes. Variations of this command include:

clear ospfv3 <*process id*> **process**
clear ospfv3 <*process id*> **redistribution**
clear ospfv3 process
clear ospfv3 redistribution

Syntax Description

<*process id*>	Optional. Restarts or resets the specified OSPFv3 process, or refreshes routes distributed only to the specified process.
process	Specifies that all OSPFv3 processes are reset and restarted.
redistribution	Specifies that all routes distributed into OSPFv3 processes are refreshed.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example resets and restarts OSPFv3 process **5**:

>**enable**
#clear ospfv3 5 process

The following example refreshes all routes distributed into OSPFv3 processes:

>**enable**
#clear ospfv3 redistribution

clear performance-statistics

Use the **clear performance-statistics** command to clear the performance monitoring statistics on a particular interface or Ethernet virtual connection (EVC). Variations of this command include:

clear performance-statistics evc <*name*>
clear performance-statistics <*interface*>

Syntax Description

evc <*name*>	Specifies an EVC on which to clear the performance statistics.
<*interface*>	Specifies the interface on which to clear the performance statistics. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear performance-statistics ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.
Release R11.2.0	Command was expanded to include the very high-speed digital subscriber line (VDSL).
Release R11.5.0	Command was expanded to include the EVC option.

Usage Examples

The following example clears all performance statistics on the Ethernet subinterface **1/1.1**:

>**enable**

#clear performance-statistics ethernet 1/1.1

clear port-security

Use the **clear port-security** command to clear the dynamic or sticky secure medium access control (MAC) addresses associated with an interface. This can be done on a per-address or per-port basis. Variations of this command include the following:

clear port-security dynamic address <*mac address*>
clear port-security dynamic interface <*interface*>
clear port-security sticky address <*mac address*>
clear port-security sticky interface <*interface*>

Syntax Description

dynamic	Clears the dynamic MAC addresses.
sticky	Clears the sticky secure MAC addresses.
address <*mac address*>	Clears the information for the specified MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
interface <*interface*>	Clears the information for the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear port-security sticky interface ?** or **clear port-security dynamic interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following command clears all dynamic secure MAC addresses associated with the Ethernet interface 0/1:

>**enable**
#clear port-security dynamic interface eth 0/1

clear port-security violation-count *<interface>*

Use the **clear port-security violation-count** command to clear the violation count associated with a particular interface.

Syntax Description

<interface>	Clears the information for the specified Ethernet interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear port-security violation-count interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following command clears the violation count associated with the Ethernet interface 0/1:

```
>enable
#clear port-security violation-count eth 0/1
```


clear pppoe

Use the **clear pppoe** command to terminate the current Point-to-Point Protocol over Ethernet (PPPoE) client session and cause AOS to attempt to re-establish the session. Variations of this command include:

clear pppoe <*interface*>
clear pppoe system-control-evc

Syntax Description

<*interface*>	Specifies the Point-to-Point Protocol (PPP) interface ID number to clear. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear pppoe ?** for a complete list of valid interfaces.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release R.10.10.0	Command was expanded to include the **system-control-evc** parameter.

Usage Examples

The following example ends the current PPPoE client session for ppp 1:

>enable
#clear pppoe 1

clear probe responder

Use the **clear probe responder** command to remove entries from the probe responders. Variations of this command include:

clear probe responder counters
clear probe responder icmp-timestamp counters
clear probe responder twamp counters
clear probe responder udp-echo counters

Syntax Description

counters	Clears the probe responder counters.
icmp-timestamp	Clears the Internet Control Message Protocol (ICMP) timestamp probe responder counters.
twamp	Clears the Two-Way Active Measurement Protocol (TWAMP) probe responder counters.
udp-echo	Clears the User Datagram Protocol (UDP) echo probe responder counters.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example removes the TWAMP responder counters:

>**enable**
#clear probe responder twamp counters

clear processes cpu max

Use the **clear processes cpu max** command to clear the maximum CPU usage statistic, which is displayed in the **show process cpu** command output.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example resets the CPU maximum usage statistics:

```
>enable
#clear processes cpu max
```

clear processes queue

Use the **clear processes queue** command to clear the contents of the system processing queues.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example clears the contents of the system processing queues:

```
>enable
#clear processes queue
```

clear qos map

Use the **clear qos map** command to clear the statistics for all defined quality of service (QoS) maps or for maps meeting user-configured specifications. Variations of this command include the following:

clear qos map
clear qos map <*name*>
clear qos map <*name*> **default**
clear qos map <*name*> <*number*>
clear qos map interface <*interface*>
clear qos map interface efm-group <*group id*>

Syntax Description

<*name*>	Optional. Clears the statistics of a defined QoS map.
<*number*>	Optional. Clears the statistics for one of the map's specified sequence numbers.
default	Optional. Clears the default QoS map entry.
efm-group <*group id*>	Specifies an Ethernet in the first mile (EFM) group ID. Range is **1** to **1024**.
interface <*interface*>	Optional. Clears QoS map statistics for the specified interface. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**.Type **clear qos map interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the **default** parameter and Ethernet interface.
Release R11.1.0	Command was expanded to include the system control Ethernet virtual connection (EVC) and system management EVC.
Release R11.4.0	Command was expanded to include the EFM group.
Release R11.9.0	Command was expanded to include the tunnel interface.

Usage Examples

The following example clears statistics for all defined QoS maps:

#clear qos map

The following example clears statistics for all entries in the **priority** QoS map:

#clear qos map priority

The following example clears statistics in entry **10** of the **priority** QoS map:

#clear qos map priority 10

The following example clears QoS statistics for a specified interface:

#clear qos map interface frame-relay 1

*The **clear counters** command clears ALL interface statistics (including QoS map interface statistics).*

clear relay

Use the **clear relay** command to reset the door contact relay.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example resets the door contact relay:

```
>enable
#clear relay
```

clear route-map counters

Use the **clear route-map counters** command to reset route map hit counters. Variations of this command include:

clear route-map counters
clear route-map counters <*name*>

Syntax Description

<*name*>	Optional. Clears the counters for the specified route map.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example clears all route map counters:

>**enable**
#clear route-map counters

clear rtp quality-monitoring

Use the **clear rtp quality-monitoring** command to clear all voice quality monitoring (VQM) statistics or only VQM statistics from the call history or a particular interface. Variations of this command include:

clear rtp quality-monitoring
clear rtp quality-monitoring call-history
clear rtp quality-monitoring interface <*interface*>

Syntax Description

call-history	Optional. Removes call statistics from the call history only.
interface <*interface*>	Optional. Clears all interface VQM statistics for the specified interface. Specifies an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear ip rtp quality-monitoring interface ?** for a valid list of interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 17.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example clears all VQM statistics from the call history:

>**enable**
#clear rtp quality-monitoring call-history

clear rtp quality-monitoring reporter

Use the **clear rtp quality-monitoring reporter** command to clear all statistics associated with all configured voice quality monitoring (VQM) reporters. Variations of this command include:

clear rtp quality-monitoring reporter
clear rtp quality-monitoring reporter <*name*>

Syntax Description

<*name*>	Optional. Clears statistics for only the specified VQM reporter.

Default Values

No default values are necessary for this command.

Command History

Release 17.6	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example clears only the statistics associated with VQM reporter **Reporter1**:

>**enable**
#clear rtp quality-monitoring reporter Reporter1

clear sip location <*username*>

Use the **clear sip location** command to clear Session Initiation Protocol (SIP) location database statistics. Variations of this command include:

clear sip location *
clear sip location <*username*>

Syntax Description

*	Clears all SIP location database statistics.
<*username*>	Clears the statistics for the specified user name.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example deletes all dynamic location entries:

```
>enable
#clear sip location *
```

clear sip resources

Use the **clear sip resources** command to clear the counters for Session Initiation Protocol (SIP) resources currently in use. Refer to *show sip on page 998* for information about using the **show sip resources** command to display the current SIP resource information.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.9	Command was introduced for AOS data products.
Release A4.01	Command was included for AOS voice products.

Usage Examples

The following example clears SIP server resource counters:

```
>enable
#clear sip resources
```


clear sip secure remote-user

Use the **clear sip secure remote-user** command to clear statistics for Session Initiation Protocol (SIP) security remote user blacklist entries and dropped requests. If you do not specify the IPv4 address for the blacklist item to clear, all blacklist items are cleared. Refer to *show sip secure remote-user on page 1004* for information about using the **show sip secure** command to display the current SIP security remote user statistics. Variations of this command include:

clear sip secure remote-user blacklist
clear sip secure remote-user blacklist *<ipv4 address>*
clear sip secure remote-user dropped-requests

Syntax Description

blacklist	Optional. Displays UDP SIP security blacklist entries.
<ipv4 address>	Optional. Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
dropped-requests	Optional. Displays UDP SIP security dropped requests due to failed authentication attempts.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example clears all entries from the SIP security remote user blacklist table:

>enable
#clear sip secure remote-user blacklist

clear sip tls session

Use the **clear sip tls session** command to clear statistics for active Session Initiation Protocol (SIP) Transport Layer Security (TLS) sessions. Variations of this command include:

clear sip tls session *
clear sip tls session <*session ID*>

Syntax Description

*****	Specifies that statistics for all TLS sessions are cleared.
<*session ID*>	Specifies that statistics for the individual TLS session are cleared. The session ID value can be determined using the command *show tls sessions on page 1053*.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example clears statistics for all TLS sessions:

>**enable**
#clear sip tls session *

clear sip trunk-registration

Use the **clear sip trunk-registration** command to clear local Session Initiation Protocol (SIP) registration information for one or more trunks. Variations of this command include:

clear sip trunk-registration
clear sip trunk-registration <*Txx*>
clear sip trunk-registration <*Txx*> <*trunk id*>

Syntax Description

<*Txx*>	Optional. Specifies the trunk to clear using its two-digit identifier (for example, **T01**).
<*trunk id*>	Optional. Clears the registration information for the specified trunk.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example clears SIP registration information for trunk 01:

>**enable**
#clear sip trunk-registration T01

clear sip user-registration

Use the **clear sip user-registration** command to clear local Session Initiation Protocol (SIP) server registration information.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example clears all SIP server registration information:

```
>enable
#clear sip user-registration
```


clear spanning-tree counters

The **clear spanning-tree counters** command clears the following counts: bridge protocol data unit (BPDU) transmit, BPDU receive, and number of transitions to forwarding state. Variations of this command include:

clear spanning-tree counters
clear spanning-tree counters interface *<interface>*

Syntax Description

interface *<interface>*	Optional. Specifies a single interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear spanning-tree counters ?** for a complete list of interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example clears the spanning tree counters for Ethernet 0/10:

>enable
#clear spanning-tree counters interface eth 0/10

clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** command to restart the protocol migration process. Variations of this command include:

clear spanning-tree detected-protocols
clear spanning-tree detected-protocols interface <*interface*>

Syntax Description

interface <*interface*>	Optional. Specifies a valid interface to clear. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear spanning-tree detected-protocols interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Functional Notes

The switch has the ability to operate using the rapid spanning-tree protocol or the legacy 802.1D version of spanning-tree. When a bridge protocol data unit (BPDU) of the legacy version is detected on an interface, the switch automatically regresses to using the 802.1D spanning-tree protocol for that interface. Issue the **clear spanning-tree detected-protocols** command to return to rapid spanning-tree operation.

Usage Examples

The following example re-initiates the protocol migration process on Ethernet interface 0/3:

```
>enable
#clear spanning-tree detected-protocols interface ethernet 0/3
```

The following example re-initiates the protocol migration process on all interfaces:

```
>enable
#clear spanning-tree detected-protocols
```


clear ssh port-forward

Use the **clear ssh port-forward** command to remove a previously defined secure shell (SSH) port forwarding. Variations of this command include:

clear ssh port-forward <*port-forward port*> <*url*>
clear ssh port-forward <*port-forward port*> <*url*> **myprivkey dsa**
clear ssh port-forward <*port-forward port*> <*url*> **password** <*password*>
clear ssh port-forward <*port-forward port*> <*url*> **port** <*port*>
clear ssh port-forward <*port-forward port*> <*url*> **port** <*port*> **myprivkey dsa**
clear ssh port-forward <*port-forward port*> <*url*> **port** <*port*> **password** <*password*>
clear ssh port-forward <*port-forward port*> <*url*> **port** <*port*> **privkey** <*filename*>
clear ssh port-forward <*port-forward port*> <*url*> **privkey** <*filename*>

Syntax Description

<*port-forward port*>	Specifies the forwarded port on the local unit.
<*url*>	Specifies the uniform resource locator (URL) of the far end listening address. The format of the URL string must be **user@server:remote-port**, for example, MGARCIA@10.10.10.1:7000. Optionally, you may include the IP address of an interface on the remote machine using the format **user@server:remote-port:FarEndListenAddress**, for example, MGARCIA@10.10.10.1:7000:10.10.10.2.
myprivkey dsa	Optional. Specifies to use the AOS unit's digital signature algorithm (DSA) private key for SSH authentication.
password <*password*>	Optional. Specifies a password to use for SSH authentication.
port <*port*>	Optional. Specifies a port to use for the underlying SSH protocol instead of the default SSH port 22. Valid range is **1** to **65535**.
privkey <*filename*>	Optional. Specifies a private key file to use for SSH authentication.

Default Values

No default values are necessary for this command.

Command History

Release 11.4.0	Command was introduced.

Usage Examples

The following example removes the forward of port **22** on the AOS device for user **MGARCIA** using port **7000** on device **10.10.10.1**:

>enable
#clear ssh port-forward 22 MGARCIA@10.10.10.1:7000 password PASSWORD

clear tacacs+ statistics

Use the **clear tacacs+ statistics** command to delete all terminal access controller access-control system plus (TACACS+) protocol statistics.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example clears all TACACS+ protocol statistics:

```
>enable
#clear tacacs+ statistics
```


clear user

Use the **clear user** command to detach a user from a given line. Variations of this command include:

clear user console <*number*>
clear user ssh <*number*>
clear user telnet <*number*>

Syntax Description

console <*number*>	Detaches a specific console user. Valid range is **0** to **1**.
ssh <*number*>	Detaches a specific secure shell (SSH) user. Valid range is **0** to **4**.
telnet <*number*>	Detaches a specific Telnet user. Valid range is **0** to **5**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example detaches the **console 1** user:

>**enable**
#clear user console 1

clear voice logging smdr

Use the **clear voice logging smdr** command to clear the local station messaging detail record (SMDR) log.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example clears the SMDR log:

```
>enable
#clear voice logging smdr
```

clear voice queue <*extension*>

Use the **clear voice queue** command to reset statistics for all call queues or the specified call queue.

Syntax Description

<*extension*>	Indicates the extension of the call queue.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example resets the statistics on the call queue on extension **6407**:

>**enable**
#clear voice queue 6407

clear vrrp counters

Use the **clear vrrp counters** command to clear the Virtual Router Redundancy Protocol (VRRP) statistics. The following are variations of this command:

clear vrrp counters
clear vrrp counters interface <*interface*>
clear vrrp counters interface <*interface*> **group** <*number*>

Syntax Description

interface <*interface*>	Optional. Clears all VRRP statistics on the specified interface. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear vrrp counters interface ?** for a complete list of valid interfaces.
group <*number*>	Optional. Clears all VRRP statistics for the specified group on the specified interface. Group numbers range from 1 to 255.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

Although VRRP group virtual router IDs (VRIDs) can be numbered between 1 and 255, only two VRRP routers per interface are supported.

Usage Examples

The following example clears all VRRP group statistics on all interfaces:

>**enable**
#clear vrrp counters

clear vrrpv3 counters

Use the **clear vrrpv3 counters** command to clear all Virtual Router Redundancy Protocol version 3 (VRRPv3) statistics. Variations of this command include:

clear vrrpv3 counters
clear vrrpv3 counters interface <*interface*>
clear vrrpv3 counters interface <*interface*> **group** <*vrid*>
clear vrrpv3 counters ipv4
clear vrrpv3 counters ipv6

Syntax Description

interface <*interface*>	Optional. Clears all VRRPv3 statistics on the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **clear vrrpv3 counters interface ?** for a complete list of valid interfaces.
group <*vrid*>	Optional. Clears all VRRPv3 statistics for the specified group virtual router ID (VRID) on the specified interface. Group VRIDs range from **1** to **255**.
ipv4	Optional. Clears all VRRPv3 statistics for the IPv4 address family.
ipv6	Optional. Clears all VRRPv3 statistics for the IPv6 address family.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.
Release R10.11.0	Command was expanded to include the **ipv4** and **ipv6** parameters.

Functional Notes

Although VRRPv3 group VRIDs can be numbered between 1 and 255, only two VRRPv3 routers per interface per IP version are supported.

Usage Examples

The following example clears all VRRPv3 group statistics on all interfaces:

>**enable**
#clear vrrpv3 counters

clear vxlan host

Use the **clear vxlan host** command to clear the remote host entries learned from the virtual extensible local area network (VxLAN) peers. Variations of this command include:

clear vxlan host <*mac address*>
clear vxlan host tunnel <*interface id*>
clear vxlan host vni <*number*>

Syntax Description

<*mac address*>	Clears host entries with the specified mac address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, 00:A0:C8:00:00:01).
tunnel <*interface id*>	Clears host entries with the specified tunnel interface. Valid interface range is **1** to **1024**.
vni <*number*>	Clears host entires with the specified VxLAN network ID (VNI). Valid range is **1** to **677215**.

Default Values

No default values are necessary for this command.

Command History

Release 13.1.0	Command was introduced.

Usage Examples

The following example clears the remote host entries for MAC address 00:A0:C8:00:00:01:

>**enable**
#clear vxlan host 00:A0:C8:00:00:01

clock auto-correct-dst

The **clock auto-correct-dst** command allows the automatic one-hour correction for daylight savings time (DST). Use the **clock no-auto-correct-dst** command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example allows for automatic DST correction:

```
>enable
#clock auto-correct-dst
```

clock no-auto-correct-dst

The **clock no-auto-correct-dst** command allows you to override the automatic one-hour correction for daylight savings time (DST).

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Functional Notes

Many time zones include an automatic one-hour correction for daylight savings time at the appropriate time. You may override it at your location using this command.

Usage Examples

The following example overrides the one-hour offset for DST:

```
>enable
#clock no-auto-correct-dst
```


clock set *<time> <day> <month> <year>*

Use the **clock set** command to configure the system software clock. For the command to be valid, all fields must be entered. Refer to the *Usage Examples* below for an example.

Syntax Description

<time>	Sets the time (in 24-hour format) of the system software clock in the format hours:minutes:seconds (HH:MM:SS).
<day>	Sets the current day of the month. Valid range is 1 to 31.
<month>	Sets the current month. Valid range is January to December. You need only enter enough characters to make the entry unique. This entry is not case sensitive.
<year>	Sets the current year. Valid range is 2000 to 2100.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sets the system software clock for 3:42 p.m., August 22, 2004:

>enable
#clock set 15:42:00 22 Au 2004

clock timezone <*value*>

The **clock timezone** command sets the unit's internal clock to the time zone of your choice. This setting is based on the difference in time (in hours) between Greenwich Mean Time (GMT) or Central Standard Time (CST) and the time zone for which you are setting up the unit. Use the **no** form of this command to disable this feature.

Syntax Description

<*value*>	Clock time zone values are specified in the *Functional Notes* section for this command.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was expanded to include the **clock timezone 0**.

clock timezone +1-Amsterdam
clock timezone +1-Belgrade
clock timezone +1-Brussels
clock timezone +1-Sarajevo
clock timezone +1-West-Africa
clock timezone +10-Brisbane
clock timezone +10-Canberra
clock timezone +10-Guam
clock timezone +10-Hobart
clock timezone +10-Vladivostok
clock timezone +11
clock timezone +12-Auckland
clock timezone +12-Fiji
clock timezone +13
clock timezone +2-Athens
clock timezone +2-Bucharest
clock timezone +2-Cairo
clock timezone +2-Harare
clock timezone +2-Helsinki
clock timezone +2-Jerusalem
clock timezone +3-Baghdad
clock timezone +3-Kuwait
clock timezone +3-Moscow
clock timezone +3-Nairobi
clock timezone +3:30
clock timezone +4-Abu-Dhabi
clock timezone +4-Baku
clock timezone +4:30
clock timezone +5-Ekaterinburg
clock timezone +5-Islamabad
clock timezone +5:30
clock timezone +5:45
clock timezone +6-Almaty
clock timezone +6-Astana
clock timezone +6-Sri-Jay
clock timezone +6:30
clock timezone +7-Bangkok
clock timezone +7-Kranoyarsk
clock timezone +8-Bejing
clock timezone +8-Irkutsk
clock timezone +8-Kuala-Lumpur
clock timezone +8-Perth
clock timezone +8-Taipei
clock timezone +9-Osaka
clock timezone +9-Seoul
clock timezone +9-Yakutsk
clock timezone +9:30-Adelaide
clock timezone +9:30-Darwin

Functional Notes

The following list shows sample cities and their time zone codes.

clock timezone -1-Azores
clock timezone -1-Cape-Verde
clock timezone -10
clock timezone -11
clock timezone -12
clock timezone -2
clock timezone -3-Brasilia
clock timezone -3-Buenos-Aires
clock timezone -3-Greenland
clock timezone -3:30
clock timezone -4-Atlantic-Time
clock timezone -4-Caracus
clock timezone -4-Santiago
clock timezone -5
clock timezone -5-Bogota
clock timezone -5-Eastern-Time
clock timezone -6-Central-America
clock timezone -6-Central-Time
clock timezone -6-Mexico-City
clock timezone -6-Saskatchewan
clock timezone -7-Arizona
clock timezone -7-Mountain-Time
clock timezone -8
clock timezone -9
clock timezone 0-Universal Coordinated Time (UTC)
clock timezone GMT-Casablanca
clock timezone GMT-Dublin

Usage Examples

The following example sets the time zone for Santiago, Chile.

>**enable**
#clock timezone -4-Santiago

configure

Use the **configure** command to enter the Global Configuration mode or to configure the system from memory. Refer to *Global Configuration Mode Command Set on page 1149* for more information. Variations of this command include:

configure memory
configure network
configure overwrite-network
configure terminal

Syntax Description

memory	Configures the active system with the commands located in the default configuration file stored in nonvolatile random access memory (NVRAM).
network	Configures the system from a Trivial File Transfer Protocol (TFTP) network host.
overwrite-network	Overwrites NVRAM memory from a TFTP network host.
terminal	Enters the Global Configuration mode.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enters the Global Configuration mode from the Enable mode:

```
>enable
#configure terminal
(config)#
```


copy

Use the **copy** command to copy the specified file from the source (flash memory) to the specified destination.

Variations of this command (valid only on AOS units WITHOUT CompactFlash®) include:

copy <*source file*> <*new file*>
copy <*source file*> **boot**
copy <*source file*> **default-config**
copy <*source file*> **fpga**
copy <*source file*> **interface** <*interface*>
copy <*source file*> **startup-config**

Syntax Description

<*source file*>	Specifies the name of the file to copy.
<*new file*>	Makes a copy of the specified source file and saves it in flash memory using the specified new name.
boot	Copies the specified source file and overwrites the boot read only memory (ROM).
default-config	Replaces the default configuration with the specified file copied from flash memory.
fpga	Updates the field-programmable gate array (FPGA) using a copy of the specified file.
interface <*interface*>	Updates the specified interface using a copy of the specified file. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **copy** <*source file*> **interface ?** to display a list of valid interfaces.
startup-config	Replaces the startup configuration with the specified file copied from flash memory.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 16.1	Command was expanded to include the **default-config**.
Release 17.2	Command was expanded to include the cellular interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Release A4.05	Command was expanded to include the asymmetric digital subscriber line (ADSL) interface.
Release A5.01	Command was expanded to include the **fpga** parameter.
Release R12.1.0	Command version **copy** <*source file*> **boot** was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

Updates to the boot ROM are required periodically to enhance and expand the unit's operation. The bootcode can be updated from within the command line interface (CLI) using the **copy** <*source file*> **boot** command.

The **copy** <*source file*> **boot** command is not available on vAOS instances.

Usage Examples

The following example copies the file **myfile.biz** (located in flash memory) and overwrites the boot ROM:

>**enable**
#copy myfile.biz boot
Upgrading bootcode is a critical process that cannot be interrupted. If something were to happen and the process was not able to be completed, it would render your unit inoperable. It is for this reason that during a bootcode upgrade, all other system tasks will be halted. This means packets will not be routed, and all console sessions will not respond during the upgrade process. Once the process finishes, the system will function as it did before. This process will take approximately 20 seconds.
Do you want to proceed? [yes/no]y

WARNING!! A bootcode upgrade has been initiated. Your session will become nonresponsive for the duration of the upgrade (approx. 20 seconds). A message will be sent when the upgrade is completed.

Bootcode upgrade process done. Your session should function normally.

Success!!!!!

copy cflash

Use the **copy cflash** command to copy files located on the CompactFlash® card to the specified destination.

The following variations of this command are valid only on AOS units with CompactFlash:

copy cflash <*source file*> **boot**
copy cflash <*source file*> **cflash** <*new file*>
copy cflash <*source file*> **flash**
copy cflash <*source file*> **flash** <*new file*>
copy cflash <*source file*> **http** <*url*>
copy cflash <*source file*> **http** <*url*> **port** <*port*>
copy cflash <*source file*> **http** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy cflash <*source file*> **http** <*url*> **username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*>
copy cflash <*source file*> **https** <*url*> **allow-tls1.0**
copy cflash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1**
copy cflash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy cflash <*source file*> **https** <*url*> **allow-tls1.1**
copy cflash <*source file*> **https** <*url*> **allow-tls1.1 allow-sslv3**
copy cflash <*source file*> **https** <*url*> **allow-sslv3**
copy cflash <*source file*> **https** <*url*> **username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **port** <*port*>
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0**
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1**
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3**
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1**
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 allow-sslv3**
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-sslv3**
copy cflash <*source file*> **https** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>

copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **https** <*url*> **port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy cflash <*source file*> **interface** <*interface*>
copy cflash <*source file*> **startup-config**
copy cflash tftp
copy cflash xmodem

Syntax Description

<*new file*>	Specifies the new file name.
<*source file*>	Specifies the name of the source file to copy.
boot	Copies the specified source file and overwrites the boot read only memory (ROM).
cflash	Specifies the location of the specified source file or the location of the new file as the CompactFlash card.
flash	Specifies the location of the source file or the location of the new file as flash memory.
http <*url*>	Specifies transferring the copied source file to an Hypertext Transfer Protocol (HTTP) server using the HTTP PUT operation. The HTTP server uniform resource locator (URL) provides the location.
https <*url*>	Specifies transferring the source file to a secure socket Hypertext Transfer Protocol Secure (HTTPS) server using the HTTPS PUT operation. The HTTPS server URL provides the location.
allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0 when transferring the source file. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS protocol version 1.1 when transferring the source file. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3 when transferring source files. If SSLv3 is enabled, then TLS version 1.0 is automatically enabled.

interface <*interface*>	Updates the specified interface using a copy of the specified file. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **copy cflash** <*source file*> **interface ?** to display a list of valid interfaces.
password <*password*>	Optional. Specifies a password for HTTP or HTTPS authentication.
port <*port*>	Optional. Specifies the port used to transfer the specified file to an HTTP or HTTPS server. Range is **0** to **65335**.
startup-config	Replaces the startup configuration with the specified file copied from the CompactFlash card.
tftp	Copies any file on the CompactFlash card to a specified Trivial File Transfer Protocol (TFTP) server. After **copy cflash tftp** is entered, the following prompts require additional information: *Address of remote host:* Specifies the IP address of the TFTP server. *Source filename:* Specifies the name of the file to copy to the TFTP server. *Destination filename:* Specifies the file name to use when storing the copied file on the TFTP server. (The file will be placed in the default directory established by the TFTP server.)
username <*username*>	Optional. Specifies a user name for HTTP or HTTPS authentication.
xmodem	Copies any file on the CompactFlash card (using the XMODEM protocol) to the terminal connected to the console port. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal. After **copy cflash xmodem** is entered, the following prompts require additional information: *Source filename:* Specifies the name of the file to copy from CompactFlash to the connected terminal.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 16.1	Command was expanded to include HTTP and HTTPS.
Release 17.2	Command was expanded to include the cellular interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Release A4.05	Command was expanded to include the asymmetric digital subscriber line (ADSL) interface.
Release R10.5.0	Command was expanded to include the **username** and **password** parameters.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example copies the source file **myfile.biz** (located on the CompactFlash card) to flash memory and names the new file **newfile.biz**:

>**enable**
#copy cflash myfile.biz flash newfile.biz

The following example creates a copy of the file **myfile.biz** (located on the CompactFlash card), names the new file **newfile.biz**, and places the new file on the installed CompactFlash card:

>**enable**
#copy cflash myfile.biz cflash newfile.biz

The following example replaces the startup configuration file with the file **newconfig.txt**:

>**enable**
#copy cflash newconfig.txt startup-config

The following example copies the file **myfile.biz** (located on the CompactFlash card) to the specified TFTP server:

>**enable**
#copy cflash tftp
Address of remote host?**10.200.2.4**
Source filename **myfile.biz**
Destination filename **myfile.biz**
Initiating TFTP transfer...
Received 45647 bytes.
Transfer Complete!

>**enable**
#copy cflash xmodem
Source filename **myfile.biz**
Begin the Xmodem transfer now...
Press CTRL+X twice to cancel
CCCCCC

AOS is now ready to transmit the file on the **CONSOLE** port (using the XMODEM protocol). The next step in the process may differ depending on the type of terminal emulation software you are using. For HyperTerminal, you will now select **Transfer > Receive File** and select the destination. Once the transfer is complete, information similar to the following is displayed:

Received 231424 bytes.
Transfer complete

copy console

Use the **copy console** command to copy the console's input to a text file. To stop copying to the text file, type **<Ctrl+D>**. The file will be saved in the AOS root directory.

Variations of this command (valid only on AOS units without CompactFlash® capability) include:

copy console *<filename>*
copy console flash *<filename>*
copy console flash *<filename>* **force-overwrite**
copy console flash startup-config
copy console flash startup-config force-overwrite
copy console startup-config
copy console startup-config force-overwrite

Variations of this command (valid only on AOS units with CompactFlash capability) include:

copy console cflash *<filename>*
copy console cflash *<filename>* **force-overwrite**

Variations of this command (valid only on AOS units with Universal Serial Bus (USB) flash drive capability) include:

copy console usbdrive0 *<filename>*
copy console usbdrive0 *<filename>* **force-overwrite**

Syntax Description

<filename>	Copies the console input and saves it to flash memory using the specified file name.
startup-config	Copies the console input and saves it to flash memory as the startup configuration.
cflash *<filename>*	Copies the console input and saves it to CompactFlash memory using the specified file name.
flash *<filename>*	Copies the console input and saves it to flash memory using the specified file name.
force-overwrite	Optional. Specifies a force override to copy the file.
usbdrive0 *<filename>*	Copies the console input and saves it to USB flash drive memory using the specified file name.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 18.2	Command was expanded to include USB flash drive memory.

Release R10.1.0	Command was expanded to include the **cflash** keyword.
Release R12.2.0	Command was expanded to include the **startup-config** parameter.

Functional Notes

The **copy console** command works much like a line editor. Prior to pressing **<Enter>**, changes can be made to the text on the line. Changes can be made using **<Delete>** and **<Backspace>** keys. The text can be traversed using the arrow keys, **<Ctrl+A>** (to go to the beginning of a line), and **<Ctrl+E>** (to go to the end of a line). To end copying to the text file, type **<Ctrl+D>.** The file will be saved in the AOS root directory. Use the **dir** command to see a list of files in the root directory.

Usage Examples

The following example copies the console input into the file **config.txt** (located in the AOS root directory):

>**enable**
#copy console flash config.txt

copy dynvoice-config

Use the **copy dynvoice-config** command to copy the dynamic voice configuration file to the specified destination.

The following variations of this command are valid only on AOS units with CompactFlash® and voice capability:

copy dynvoice-config cflash <*filename*>
copy dynvoice-config flash <*filename*>
copy dynvoice-config http <*url*>
copy dynvoice-config http <*url*> **port** <*port*>
copy dynvoice-config http <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy dynvoice-config http <*url*> **username** <*username*> **password** <*password*>
copy dynvoice-config https <*url*>
copy dynvoice-config https <*url*> **port** <*port*>
copy dynvoice-config https <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy dynvoice-config https <*url*> **username** <*username*> **password** <*password*>
copy dynvoice-config running-config
copy dynvoice-config tftp
copy dynvoice-config xmodem

Syntax Description

cflash <*filename*>	Copies the dynamic voice configuration file and saves it to the CompactFlash card using the specified file name.
flash <*filename*>	Copies the dynamic voice configuration file and saves it to flash memory using the specified file name.
http <*url*>	Specifies the Hypertext Transfer Protocol (HTTP) server uniform resource locator (URL) to which to transfer the dynamic voice configuration file using the HTTP PUT operation.
https <*url*>	Specifies the secure socket Hypertext Transfer Protocol (HTTPS) server uniform resource locator (URL) to which to transfer the dynamic voice configuration file using the HTTPS PUT operation.
password <*password*>	Optional. Specifies a password for HTTP or HTTPS authentication.
port <*port*>	Optional. Specifies the port used to transfer the specified file to an HTTP or HTTPS server. Range is **0** to **65335**.
running-config	Replaces the active running configuration with a copy of the dynamic voice configuration file.
tftp	Specifies the Trivial File Transfer Protocol (TFTP) server to which to copy the dynamic voice configuration file. After **copy dynvoice-config tftp** is entered, the following prompts require additional information: *Address of remote host:* Specifies the IP address of the TFTP server. *Source filename:* Specifies the name of the file (located on the CompactFlash card) to copy to the TFTP server.

	Destination filename:	Specifies the file name to use when storing the copied file on the TFTP server. The file will be placed in the default directory established by the TFTP server.
username <*username*>	Optional. Specifies a user name for HTTP or HTTPS authentication.	
xmodem	Copies the dynamic voice configuration file (using the XMODEM protocol) and saves it to the terminal connected to the console port. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal. After **copy dynvoice-config xmodem** is entered, the following prompts require additional information:	
	Source filename:	Specifies the name of the file to copy from CompactFlash to the connected terminal.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 16.1	Command was expanded to include the **http** parameter.
Release R10.5.0	Command was expanded to include the **https**, **port**, **username**, and **password** parameters.

Usage Examples

The following example copies the dynamic voice configuration file and saves it to the CompactFlash card using the name **myvoice-config**:

>**enable**
#copy dynvoice-config cflash myvoice-config
Percent Complete 100%

The following example copies the dynamic voice configuration file and saves it to flash memory using the name **myvoice-config**:

>**enable**
#copy dynvoice-config flash myvoice-config
Percent Complete 100%

The following example replaces the active running configuration with a copy of the dynamic voice configuration file:

>**enable**
#copy dynvoice-config running-config
Percent Complete 100%

The following example copies the dynamic voice configuration file and saves it to the TFTP server:

>**enable**
#copy dynvoice-config tftp
Address of remote host? **10.200.2.4**
Destination filename? **myvoice-config**
Initiating TFTP transfer...
Sent 5221 bytes.
Transfer complete.

copy flash

Use the **copy flash** command to copy files located in flash memory to a specified destination. Certain variations of this command are available only on specific AOS units and are explained below.

The following variations of this command are valid on all AOS units:

copy flash <*source file*> **http** <*url*> **port** <*port*>
copy flash <*source file*> **http** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy flash <*source file*> **http** <*url*> **username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*>
copy flash <*source file*> **https** <*url*> **allow-tls1.0**
copy flash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1**
copy flash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy flash <*source file*> **https** <*url*> **allow-tls1.0 allow-sslv3**
copy flash <*source file*> **https** <*url*> **allow-tls1.1**
copy flash <*source file*> **https** <*url*> **allow-tls1.1 allow-sslv3**
copy flash <*source file*> **https** <*url*> **allow-sslv3**
copy flash <*source file*> **https** <*url*> **username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **allow-sslv3 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **port** <*port*>
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0**
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1**
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3**
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1**
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 allow-sslv3**
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-sslv3**
copy flash <*source file*> **https** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>

copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy flash <*source file*> **https** <*url*> **port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy flash <*source file*> **scp** <*url*>
copy flash <*source file*> **scp** <*url*> myprivkey <*private key for authentication*>
copy flash <*source file*> **scp** <*url*> **myprivkey dsa**
copy flash <*source file*> **scp** <*url*> **myprivkey ecdsa256**
copy flash <*source file*> **scp** <*url*> **myprivkey ecdsa384**
copy flash <*source file*> **scp** <*url*> **myprivkey ecdsa521**
copy flash <*source file*> **scp** <*url*> **myprivkey rsa**
copy flash <*source file*> **scp** <*url*> **myprivkey rsa-sha2-512**
copy flash <*source file*> **scp** <*url*> **privkey** <*filename*>
copy flash <*source file*> **scp** <*url*> **password** <*password*>
copy flash <*source file*> **scp** <*url*> **port** <*port*>
copy flash <*source file*> **scp** <*url*> **port** <*port*> **myprivkey** <*private key for authentication*>
copy flash <*source file*> **scp** <*url*> **port** <*port*> **myprivkey dsa**
copy flash <*source file*> **scp** <*url*> **port** <*port*> **myprivkey ecdsa256**
copy flash <*source file*> **scp** <*url*> **port** <*port*> **myprivkey ecdsa384**
copy flash <*source file*> **scp** <*url*> **port** <*port*> **myprivkey ecdsa521**
copy flash <*source file*> **scp** <*url*> **port** <*port*> **myprivkey rsa**
copy flash <*source file*> **scp** <*url*> **port** <*port*> **myprivkey rsa-sha2-512**
copy flash <*source file*> **scp** <*url*> **port** <*port*> **privkey** <*private key for authentication*>
copy flash <*source file*> **scp** <*url*> **port** <*port*> **password** <*password*>
copy flash <*source file*> **sftp** <*url*>
copy flash <*source file*> **sftp** <*url*> **myprivkey** <*private key for authentication*>
copy flash <*source file*> **sftp** <*url*> **myprivkey dsa**
copy flash <*source file*> **sftp** <*url*> **myprivkey ecdsa256**
copy flash <*source file*> **sftp** <*url*> **myprivkey ecdsa384**
copy flash <*source file*> **sftp** <*url*> **myprivkey ecdsa521**
copy flash <*source file*> **sftp** <*url*> **myprivkey rsa**
copy flash <*source file*> **sftp** <*url*> **myprivkey rsa-sha2-512**
copy flash <*source file*> **sftp** <*url*> **privkey** <*private key for authentication*>
copy flash <*source file*> **sftp** <*url*> **password** <*password*>
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **myprivkey** <*private key for authentication*>
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **myprivkey dsa**
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **myprivkey ecdsa256**
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **myprivkey ecdsa384**
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **myprivkey ecdsa521**
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **myprivkey rsa**
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **myprivkey rsa-sha2-512**
copy flash <*source file*> **sftp** <*url*> **port** <*port*> **privkey** <*filename*>
copy flash <*source file*> **sftp** <*url*> **port password** <*password*>
copy flash tftp

copy flash xmodem
copy flash <*filename*>

The following variations of this command are valid only on AOS units with CompactFlash® capability:

copy flash <*source file*> **boot**
copy flash <*source file*> **cflash**
copy flash <*source file*> **cflash** <*new file*>
copy flash <*source file*> **flash** <*new file*>
copy flash <*source file*> **interface** <*interface*>
copy flash <*source file*> **startup-config**

The following variations of this command are valid only on AOS units with CompactFlash and voice capability:

copy flash <*source file*> **dynvoice-config**

The following variations of this command are valid only on AOS units with **ramdisk** enabled:

copy flash <*source file*> **ramdisk**
copy flash <*source file*> **ramdisk** <*new file*>

The following variations of this command are valid only on AOS units with Universal Serial Bus (USB) flash drive capability:

copy flash <*source file*> **usbdrive0**
copy flash <*source file*> **usbdrive0** <*new file*>

The following variations of this command are valid only on AOS units with field-programmable gate arrays (FPGAs):

copy flash <*source file*> **fpga**

Syntax Description

<*new file*>	Saves the file using the specified file name.
<*source file*>	Specifies the name of the file to copy.
boot	Copies the specified source file and overwrites the boot read only memory (ROM).
cflash	Copies a file and saves it to the CompactFlash card.
dynvoice-config	Replaces the dynamic voice configuration file with the specified file copied from flash memory.
flash	Copies the specified file and saves it to flash memory.
fpga	Copies the specified file and saves it as the FPGA image.
http <*url*>	Specifies the Hypertext Transfer Protocol (HTTP) server uniform resource locator (URL) to which to transfer the source file using the HTTP PUT operation.

https <*url*>	Specifies the secure socket Hypertext Transfer Protocol (HTTPS) server uniform resource locator (URL) to which to transfer the source file using the HTTPS PUT operation.
allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0 when transferring the source file. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS protocol version 1.1 when transferring the source file. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3 when transferring source files. If SSLv3 is enabled, then TLS version 1.0 is automatically enabled.
interface <*interface*>	Updates the specified interface using a copy of the specified file. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **copy flash** <*source file*> **interface ?** to display a list of valid interfaces.
myprivkey	Optional. Specifies the AOS unit's private key is used for SSH authentication.
dsa	Optional. Specifies to use the unit's Digital Signature Algorithm (DSA) private key for SSH authentication.
rsa	Optional. Specifies to use the unit's Rivest-Shamir-Adleman (RSA) private key for SSH authentication.
ecdsa	Optional. Specifies to use the unit's ECDSA nistp256|384|521 private key for SSH authentication.
password <*password*>	Optional. Specifies a password for HTTP, HTTPS, or SSH authentication.
port <*port*>	Optional. Specifies the port used to transfer the specified file to an HTTP, HTTPS, server. Range is **0** to **65335**.
privkey <*filename*>	Optional. Specifies the filename of a 3rd party private key file for SSH authentication in privacy enhanced email (PEM) format.
ramdisk	Copies a file and saves it to the volatile RAM disk.
scp <*url*>	Specifies the Secure Copy Protocol (SCP) server Uniform Resource Locator (URL) to which to transfer the source file. Specify the URL in the following format:**user@server:/path/filename.**
sftp <*url*>	Specifies the Secure File Transfer Protocol server Uniform Resource Locator (URL) to which to transfer the source file. Specify the URL in the following format:**user@server:/path/filename.**
startup-config	Replaces the startup configuration file with a copy of the specified file.
tftp	Copies any file located in flash memory to a specified Trivial File Transfer Protocol (TFTP) server. After **copy flash tftp** is entered, the following prompts require additional information: *Address of remote host:* Specifies the IP address of the TFTP server.

	Source filename:	Specifies the name of the file (located in flash memory) to copy to the TFTP server.
	Destination filename:	Specifies the file name to use when storing the copied file on the TFTP server. The file will be placed in the default directory established by the TFTP server.
usbdrive0	Specifies saving the file to USB flash drive memory.	
username <*username*>	Optional. Specifies a user name for HTTP or HTTPS authentication.	
xmodem	Copies any file located in flash memory (using the XMODEM protocol) to the terminal connected to the console port. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal.	
	After **copy flash xmodem** is entered, the following prompts require additional information:	
	Source filename:	Specifies the name of the file to copy from system flash memory using XMODEM.

Default Values

No default values are necessary for this command.

Command History

Release R14.4.0	Added **copy flash scp** and **sftp** options from local to remote server **with vrf** and **without vrf**.

Functional Notes

The **myprivkey** keyword specifies to use the unit's private key for SSH authentication. This is the key generated using the command **ssh key regenerate sftp**. Use the **privkey** keyword if you are using 3rd party keys instead of the keys generated by the unit.

Usage Examples

The following example creates a copy of the file **myfile.biz** (located in flash memory), names the new file **newfile.biz**, and places the new file in flash memory:

```
>enable
#copy flash myfile.biz flash newfile.biz
```

The following example copies the file **myfile.biz** (located in flash memory) to CompactFlash memory and names the new file **newfile.biz**:

```
>enable
#copy flash myfile.biz cflash newfile.biz
```

The following example copies the file **new_startup_config.txt** (located in flash memory) to the startup configuration:

```
>enable
#copy flash new_startup_config.txt startup-config
```

The following example copies the file **myfile.biz** (located in flash memory) to a TFTP server:

>**enable**
#copy flash tftp
Address of remote host? **10.200.2.4**
Source filename? **myfile.biz**
Destination filename? **myfile.biz**
Initiating TFTP transfer...
Sent 769060 bytes.
Transfer Complete!

The following example copies the file **startup-config.txt** to the SSH server **adtran@10.200.2.4:/backup/start** using a DSA private key generated in AOS.

>**enable**
#copy flash startup-config.txt sftp adtran@10.200.2.4:/backup/start myprivkey dsa
Initiating SFTP transfer...
Transferred 5510 bytes in 1 secs. (5.380 KB/sec)
Transfer complete.

The following example copies the file **myfile.biz** (located in flash memory) to USB flash drive memory and names the new file **newfile.biz**:

>**enable**
#copy flash myfile.biz usbdrive0 newfile.biz

The following example copies the file **myfile.biz** (located in flash memory) to the connected terminal using XMODEM protocol:

>**enable**
#copy flash xmodem
Source filename? **myfile.biz**
Begin the Xmodem transfer now...
Press CTRL+X twice to cancel
CCCCCC

AOS is now ready to transmit the file on the **CONSOLE** port (using the XMODEM protocol). The next step in the process may differ depending on the type of terminal emulation software you are using. For HyperTerminal, you will now select **Transfer > Receive File** and select the destination. Once the transfer is complete, information similar to the following is displayed:

Sent 231424 bytes.
Transfer complete

copy http

Use the **copy http** command to copy a file located on a network Hypertext Transfer Protocol (HTTP) server to a specified destination. Certain variations of this command are available only on specific AOS units and are explained below.

The following variations of this command are valid on all AOS units:

copy http <*url*> **flash** <*destination file*>
copy http <*url*> **flash** <*destination file*> **username** <*username*> **password** <*password*>
copy http <*url*> **flash** <*destination file*> **force-overwrite**
copy http <*url*> **flash** <*destination file*> **force-overwrite port** <*port*>
copy http <*url*> **flash** <*destination file*> **force-overwrite port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **flash** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy http <*url*> **flash** <*destination file*> **port** <*port*>
copy http <*url*> **flash** <*destination file*> **port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **running-config**
copy http <*url*> **running-config username** <*username*> **password** <*password*>
copy http <*url*> **running-config port** <*port*>
copy http <*url*> **running-config port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **startup-config**
copy http <*url*> **startup-config username** <*username*> **password** <*password*>
copy http <*url*> **startup-config port** <*port*>
copy http <*url*> **startup-config port** <*port*> **username** <*username*> **password** <*password*>

The following variations of this command are valid only on AOS units with CompactFlash® capability:

copy http <*url*> **cflash** <*destination file*> **username** <*username*> **password** <*password*>
copy http <*url*> **cflash** <*destination file*>
copy http <*url*> **cflash** <*destination file*> **force-overwrite**
copy http <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*>
copy http <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **cflash** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy http <*url*> **cflash** <*destination file*> **port** <*port*>
copy http <*url*> **cflash** <*destination file*> **port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **cflash running-config**
copy http <*url*> **cflash running-config port** <*port*>

The following variations of this command are valid only on AOS units with CompactFlash and voice capability:

copy http <*url*> **dynvoice-config**
copy http <*url*> **dynvoice-config port** <*port*>
copy http <*url*> **dynvoice-config port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **dynvoice-config username** <*username*> **password** <*password*>

The following variations of this command are valid only on AOS units with **ramdisk** enabled:

copy http <*url*> **ramdisk** <*destination file*>
copy http <*url*> **ramdisk** <*destination file*> **username** <*username*> **password** <*password*>
copy http <*url*> **ramdisk** <*destination file*> **force-overwrite**
copy http <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*>
copy http <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **ramdisk** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy http <*url*> **ramdisk** <*destination file*> **port** <*port*>
copy http <*url*> **ramdisk** <*destination file*> **port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **ramdisk running-config**
copy http <*url*> **ramdisk running-config port** <*port*>

The following variations of this command are valid only on AOS units with Universal Serial Bus (USB) flash drive capability:

copy http <*url*> **usbdrive0** <*destination file*>
copy http <*url*> **usbdrive0** <*destination file*> **username** <*username*> **password** <*password*>
copy http <*url*> **usbdrive0** <*destination file*> **force-overwrite**
copy http <*url*> **usbdrive0** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy http <*url*> **usbdrive0** <*destination file*> **force-overwrite port** <*port*>
copy http <*url*> **usbdrive0** <*destination file*> **force-overwrite port** <*port*> **username** <*username*> **password** <*password*>
copy http <*url*> **usbdrive0** <*destination file*> **port** <*port*>
copy http <*url*> **usbdrive0** <*destination file*> **port** <*port*> **username** <*username*> **password** <*password*>

Syntax Description

<*destination file*>	Specifies the new name of the file after it is copied.
cflash	Copies a file from the HTTP server to the CompactFlash card.
dynvoice-config	Specifies that the file copied from the HTTP server overwrite the dynamic voice configuration file.
flash	Specifies the flash memory as the destination for the copied file.
force-overwrite	Optional. Specifies a force override to copy the file.
http <*url*>	Specifies the URL of the HTTP server.
password <*password*>	Optional. Specifies a password for HTTP authentication.
port <*port*>	Optional. Specifies the port used to transfer the specified file from an HTTP server. Range is **0** to **65335**.
ramdisk	Copies a file from the HTTP server to the volatile RAM disk.
running-config	Replaces the active running configuration file with the file copied from the HTTP server.
startup-config	Replaces the startup configuration file with the file copied from the HTTP server.

username <*username*>	Optional. Specifies a user name for HTTP authentication.
usbdrive0	Specifies the USB flash drive memory as the destination for the copied file.

Default Values

By default, the **port** value is **80**.

Command History

Release 16.1	Command was introduced.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include the USB flash drive memory.
Release R10.5.0	Command was expanded to include the **username** and **password** parameters.

Usage Examples

The following example replaces the current running configuration file with **newconfig.txt** from the HTTP server (**10.200.2.4**):

```
#copy http http://10.200.2.4/newconfig.txt running-config
Initiating HTTP transfer...
Received 4562 bytes.
Transfer Complete!
#
```

The following example copies the file **myfile.biz** from the HTTP server (**10.200.2.4**) and saves it to CompactFlash memory (naming the copy **newfile.biz**):

```
#copy http http://10.200.2.4/SomeDirectory/AnotherDirectory/myfile.biz cflash newfile.biz
Initiating HTTP transfer...
Received 45647 bytes.
Transfer Complete!
```

copy https

Use the **copy https** command to copy a file located on a secure socket Hypertext Transfer Protocol Secure (HTTPS) server to a specified destination using the HTTPS PUT operation. Certain variations of this command are available only on specific AOS units and are explained below.

The following variations of this command are valid on all AOS units:

copy https <*url*> **flash** <*destination file*>
copy https <*url*> **flash** <*destination file*> **allow-tls1.0**
copy https <*url*> **flash** <*destination file*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **flash** <*destination file*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **flash** <*destination file*> **allow-tls1.0 allow-sslv3**
copy https <*url*> **flash** <*destination file*> **allow-tls1.1**
copy https <*url*> **flash** <*destination file*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **flash** <*destination file*> **allow-sslv3**
copy https <*url*> **flash** <*destination file*> **username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **force-overwrite**
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0**
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1**
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0 allow-sslv3**
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.1**
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.1 allow-sslv3**
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-sslv3**
copy https <*url*> **flash** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **force-overwrite allow-tls1.1 username** <*username*> **password**

<password>
copy https *<url>* **flash** *<destination file>* **force-overwrite allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0**
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0 allow-tls1.1**
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0 allow-sslv3**
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.1**
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.1 allow-sslv3**
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-sslv3**
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0 allow-tls1.1 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.0 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.1 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **force-overwrite port** *<port>* **allow-sslv3 username** *<username>* **password** *<password>*

copy https *<url>* **flash** *<destination file>* **port** *<port>*
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.0**
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.0 allow-tls1.1**
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.0 allow-sslv3**
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.1**
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.1 allow-sslv3**
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-sslv3**
copy https *<url>* **flash** *<destination file>* **port** *<port>* **username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.0 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.0 allow-tls1.1 username** *<username>* **password** *<password>*
copy https *<url>* **flash** *<destination file>* **port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*

copy https <*url*> **flash** <*destination file*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **flash** <*destination file*> **port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **running-config**
copy https <*url*> **running-config allow-tls1.0**
copy https <*url*> **running-config allow-tls1.0 allow-tls1.1**
copy https <*url*> **running-config allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **running-config allow-tls1.0 allow-sslv3**
copy https <*url*> **running-config allow-tls1.1**
copy https <*url*> **running-config allow-tls1.1 allow-sslv3**
copy https <*url*> **running-config allow-sslv3**
copy https <*url*> **running-config username** <*username*> **password** <*password*>
copy https <*url*> **running-config allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **running-config allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **running-config allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **running-config allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **running-config allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **running-config allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **running-config allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **running-config port** <*port*>
copy https <*url*> **running-config port** <*port*> **allow-tls1.0**
copy https <*url*> **running-config port** <*port*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **running-config port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **running-config port** <*port*> **allow-tls1.0 allow-sslv3**
copy https <*url*> **running-config port** <*port*> **allow-tls1.1**
copy https <*url*> **running-config port** <*port*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **running-config port** <*port*> **allow-sslv3**
copy https <*url*> **running-config port** <*port*> **username** <*username*> **password** <*password*>
copy https <*url*> **running-config port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **running-config port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **running-config port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **running-config port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **running-config port** <*port*> **allow-tls1.1 username** <*username*> **password**

<password>
copy https *<url>* **running-config port** *<port>* **allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **running-config port** *<port>* **allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config**
copy https *<url>* **startup-config allow-tls1.0**
copy https *<url>* **startup-config allow-tls1.0 allow-tls1.1**
copy https *<url>* **startup-config allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https *<url>* **startup-config allow-tls1.0 allow-sslv3**
copy https *<url>* **startup-config allow-tls1.1**
copy https *<url>* **startup-config allow-tls1.1 allow-sslv3**
copy https *<url>* **startup-config allow-sslv3**
copy https *<url>* **startup-config username** *<username>* **password** *<password>*
copy https *<url>* **startup-config allow-tls1.0 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config allow-tls1.0 allow-tls1.1 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config allow-tls1.0 allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config allow-tls1.0 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config allow-tls1.1 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config port** *<port>*
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0**
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0 allow-tls1.1**
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0 allow-sslv3**
copy https *<url>* **startup-config port** *<port>* **allow-tls1.1**
copy https *<url>* **startup-config port** *<port>* **allow-tls1.1 allow-sslv3**
copy https *<url>* **startup-config port** *<port>* **allow-sslv3**
copy https *<url>* **startup-config port** *<port>* **username** *<username>* **password** *<password>*
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0 allow-tls1.1 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config port** *<port>* **allow-tls1.0 allow-sslv3 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config port** *<port>* **allow-tls1.1 username** *<username>* **password** *<password>*
copy https *<url>* **startup-config port** *<port>* **allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*

copy https <*url*> **startup-config port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>

The following variations of this command are valid only on AOS units with CompactFlash® capability:

copy https <*url*> **cflash** <*destination file*>
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0**
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite**
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0**
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>

copy https <*url*> **cflash** <*destination file*> **force-overwrite allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0**
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **force-overwrite port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.0**
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tsl1.0 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.1**
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-sslv3**
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>

copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash** <*destination file*> **port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **cflash running-config**
copy https <*url*> **cflash running-config port** <*port*>

The following variations of this command are valid only on AOS units with CompactFlash and voice capability:

copy https <*url*> **dynvoice-config**
copy https <*url*> **dynvoice-config port** <*port*>
copy https <*url*> **dynvoice-config port** <*port*> **username** <*username*> **password** <*password*>
copy https <*url*> **dynvoice-config username** <*username*> **password** <*password*>

The following variations of this command are valid only on AOS units with **ramdisk** enabled:

copy https <*url*> **ramdisk** <*destination file*>
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0**
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.1**
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0 username** <*username*> **password** <*password*>

copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **force-overwrite port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0**
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1**
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.1**
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.1 allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-sslv3**
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **username** <*username*> **password** <*password*>

copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk** <*destination file*> **port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy https <*url*> **ramdisk running-config**
copy https <*url*> **ramdisk running-config port** <*port*>

The following variations of this command are valid only on AOS units with Universal Serial Bus (USB) flash drive capability:

copy https <*url*> **usbdrive0** <*destination file*>
copy https <*url*> **usbdrive0** <*destination file*> **username** <*username*> **password** <*password*>
copy https <*url*> **usbdrive0** <*destination file*> **force-overwrite**
copy https <*url*> **usbdrive0** <*destination file*> **force-overwrite username** <*username*> **password** <*password*>
copy https <*url*> **usbdrive0** <*destination file*> **force-overwrite port** <*port*>
copy https <*url*> **usbdrive0** <*destination file*> **force-overwrite port** <*port*> **username** <*username*> **password** <*password*>
copy https <*url*> **usbdrive0** <*destination file*> **port** <*port*>
copy https <*url*> **usbdrive0** <*destination file*> **port** <*port*> **username *<username>* password *<password>***

Syntax Description

allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0 when copying the file. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS protocol version 1.1 when copying the file. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3 when copying the file. If SSLv3 is enabled, then TLS version 1.0 is automatically enabled.
<*destination file*>	Specifies the new name of the file after it is copied.
cflash	Specifies the CompactFlash card as the destination for the copied file.
dynvoice-config	Specifies that the file copied from the HTTP secure server overwrite the dynamic voice configuration file.
flash	Specifies the flash memory as the destination for the copied file.

force-overwrite	Optional. Specifies a force override to copy the file.
https <*url*>	Specifies the URL of the HTTP secure server.
password <*password*>	Optional. Specifies a password to use with HTTPS authentication.
port <*port*>	Optional. Specifies the port used to transfer the specified file from an HTTP secure server. Range is **0** to **65335**.
ramdisk	Specifies the volatile RAM disk as the destination for the copied file.
running-config	Replaces the active running configuration with the file copied from the HTTP secure server.
startup-config	Replaces the startup configuration file with the file copied from the HTTP secure server.
usbdrive0	Specifies the USB flash drive memory as the destination for the copied file.
username <*username*>	Optional. Specifies a user name to use with HTTPS authentication.

Default Values

By default, the **port** value is **443**.

Command History

Release 16.1	Command was introduced.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include USB flash drive memory.
Release R10.5.0	Command was expanded to include the **password** and **username** parameters.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example replaces the current running configuration file with **newconfig.txt** from the HTTPS server (**MyWebServer**):

```
#copy https https://MyWebServer.com/newconfig.txt running-config
Initiating HTTPS transfer...
Received 4562 bytes.
Transfer Complete!
#
```

The following example copies the file **myfile.biz** from the HTTPS server (**10.200.2.4**) and saves it to CompactFlash memory (naming the copy **newfile.biz**):

```
#copy https https://10.200.2.4/myfile.biz cflash newfile.biz
Initiating HTTPS transfer...
Received 45647 bytes.
Transfer Complete!
```


copy ramdisk

Use the **copy ramdisk** command to copy files located in the volatile RAM disk memory to a specified destination. Variations of this command include:

copy ramdisk <*source file*> **flash**
copy ramdisk <*source file*> **flash** <*new file*>
copy ramdisk <*source file*> **http** <*url*>
copy ramdisk <*source file*> **http** <*url*> **username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **http** <*url*> **port** <*port*>
copy ramdisk <*source file*> **http** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*>
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0**
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1**
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0 allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.1**
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.1 allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **allow-sslv3 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0**
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1**
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1**
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-sslv3**
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*>

password <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **https** <*url*> **port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
copy ramdisk <*source file*> **overwrite primary**
copy ramdisk <*source file*> **overwrite primary verify**
copy ramdisk <*source file*> **overwrite secondary**
copy ramdisk <*source file*> **overwrite secondary verify**
copy ramdisk tftp
copy ramdisk xmodem

Not all units are capable of using a RAM disk file system. Use the ***copy ?*** *command to display a list of valid commands at the enable prompt.*

Syntax Description

<*new file*>	Specifies the new file name.
<*source file*>	Specifies the name of the source file to copy.
flash	Specifies the location to copy the new file as the system flash memory.
http <*url*>	Specifies the Hypertext Transfer Protocol (HTTP) server uniform resource locator (URL) to which to transfer the source file using the HTTP PUT operation.
https <*url*>	Specifies the secure socket Hypertext Transfer Protocol (HTTPS) server uniform resource locator (URL) to which to transfer the source file using the HTTPS PUT operation.
allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0 when transferring the source file. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS protocol version 1.1 when transferring the source file. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3 when transferring the source file. If SSLv3 is enabled, then TLS version 1.0 is automatically enabled.
overwrite primary	Replaces the primary boot image file with the file from RAM disk. The file to be overwritten is deleted prior to copying the new file. In order for this command to succeed, the RAM disk must be mounted, the specified file must exist, and the specified file must verify with a valid signature for the unit.

overwrite secondary	Replaces the secondary boot image file with the file from RAM disk. The file to be overwritten is deleted prior to copying the new file. In order for this command to succeed, the RAM disk must be mounted, the specified file must exist, and the specified file must verify with a valid signature for the unit.
password <*password*>	Optional. Specifies a password for HTTP or HTTPS authentication.
port <*port*>	Optional. Specifies the port used to transfer the specified file to an HTTP or HTTPS server. Range is **0** to **65335**.
tftp	Copies the specified file from the RAM disk to a specified Trivial File Transfer Protocol (TFTP) server. After the command is entered, the following prompts require additional information: *Address of remote host:* Specifies the IP address of the TFTP server. *Source filename:* Specifies the name of the file (located on the RAM disk) to copy to the TFTP server. *Destination filename:* Specifies the file name to use when storing the copied file on the TFTP server. The file will be placed in the default directory established by the TFTP server.
username <*username*>	Optional. Specifies a user name to use with HTTP or HTTPS authentication.
verify	Optional. Specifies that a second verification of the new primary or secondary boot system image is performed after it is copied.
xmodem	Copies the specified file from the RAM disk (using the XMODEM protocol) to the terminal connected to the console port. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal. After the command is entered, the following prompts require additional information: *Source filename:* Specifies the name of the file (located on the RAM disk) to copy using XMODEM.

Default Values

No default values are necessary for this command.

Command History

Release 17.7	Command was introduced.
Release R10.5.0	Command was expanded to include the following parameters: **http**, **https**, **port**, **username**, and **password**.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example creates a copy of the file **myfile.biz** (located on the RAM disk), names the new file **newfile.biz**, and places the new file in flash memory:

>**enable**
#copy ramdisk myfile.biz flash newfile.biz

The following example copies the software file **myfile.biz** (located on the RAM disk) to a TFTP server:

>**enable**
#copy ramdisk tftp
Address of remote host? **10.200.2.4**
Source filename? **myfile.biz**
Destination filename? **myfile.biz**
Initiating TFTP transfer...
Sent 769060 bytes.
Transfer Complete!
The following example copies the software file **myfile.biz** (located on the RAM disk) to the connected terminal using XMODEM protocol:

>**enable**
#copy ramdisk xmodem
Source filename? **myfile.biz**
Begin the Xmodem transfer now...
Press CTRL+X twice to cancel
CCCCCC

AOS is now ready to transmit the file on the **CONSOLE** port (using the XMODEM protocol). The next step in the process may differ depending on the type of terminal emulation software you are using. For HyperTerminal, you will now select **Transfer > Receive File** and select the destination. Once the transfer is complete, information similar to the following is displayed:

Sent 231424 bytes.
Transfer complete

copy running-config

Use the **copy running-config** command to create a copy of the current running configuration and replace the current startup configuration or save it to a specified location. Certain variations of this command are available only on specific AOS units and are explained below.

The following variations of this command are valid on all AOS units:

copy running-config <*filename*>
copy running-config http <*url*>
copy running-config http <*url*> **username** <*username*> **password** <*password*>
copy running-config http <*url*> **port** <*port*>
copy running-config http <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy running-config https <*url*>
copy running-config https <*url*> **allow-tls1.0**
copy running-config https <*url*> **allow-tls1.0 allow-tls1.1**
copy running-config https <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy running-config https <*url*> **allow-tls1.0 allow-sslv3**
copy running-config https <*url*> **allow-tls1.1**
copy running-config https <*url*> **allow-tls1.1 allow-sslv3**
copy running-config https <*url*> **allow-sslv3**
copy running-config https <*url*> **username** <*username*> **password** <*password*>
copy running-config https <*url*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy running-config https <*url*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy running-config https <*url*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy running-config https <*url*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy running-config https <*url*> **allow-sslv3 username** <*username*> **password** <*password*>
copy running-config https <*url*> **port** <*port*>
copy running-config https <*url*> **port** <*port*> **allow-tls1.0**
copy running-config https <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1**
copy running-config https <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy running-config https <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3**
copy running-config https <*url*> **port** <*port*> **allow-sslv3**
copy running-config https <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy running-config https <*url*> **port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
copy running-config https <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
copy running-config https <*url*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
copy running-config https <*url*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
copy running-config https <*url*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>

copy running-config https *<url>* **port** *<port>* **allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy running-config https *<url>* **port** *<port>* **allow-sslv3 username** *<username>* **password** *<password>*
copy running-config tftp
copy running-config xmodem

The following variations of this command are valid only on AOS units with CompactFlash® capability:

copy running-config cflash *<filename>*
copy running-config cflash startup-config
copy running-config flash *<filename>*
copy running-config flash startup-config

The following variations of this command are valid only on AOS units with CompactFlash and voice capability:

copy running-config dynvoice-config
copy running-config dynvoice-config tftp
copy running-config dynvoice-config http *<url>*
copy running-config non-dynvoice-config http *<url>*

The following variations of this command are valid only on AOS units with **ramdisk** enabled:

copy running-config ramdisk *<filename>*

The following variations of this command are valid only on AOS units with Universal Serial Bus (USB) flash drive capability:

copy running-config usbdrive0 *<filename>*
copy running-config usbdrive0 startup-config

Syntax Description

<filename>	Specifies the filename to use when saving the configuration file.
cflash	Specifies the location so save the current running configuration as the CompactFlash card.
dynvoice-config	Copies the current active voice running configuration and saves it to the dynamic voice configuration file.
flash	Specifies saving the current running configuration to flash memory.
http *<url>*	Specifies the Hypertext Transfer Protocol (HTTP) server uniform resource locator (URL) to which to transfer the configuration file using the HTTP PUT operation.
https *<url>*	Specifies the secure socket Hypertext Transfer Protocol (HTTPS) server uniform resource locator (URL) to which to transfer the configuration file using the HTTPS PUT operation.

allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0 when transferring the configuration file. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS version 1.1 when transferring the configuration file. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3 when transferring the configuration file. If SSLv3 is enabled, then TLS version 1.0 is automatically enabled.
non-dynvoice-config	Copies the current nondynamic portion of the voice running configuration and saves it to the nondynamic voice configuration file.
password <*password*>	Optional. Specifies a password for HTTP or HTTPS authentication.
port <*port*>	Optional. Specifies the port used to transfer the specified file to an HTTP or HTTPS server. Range is **0** to **65335**.
ramdisk	Copies the current running configuration to the volatile RAM disk.
startup-config	Replaces the startup configuration (located in either CompactFlash or system flash) with a copy of the current running configuration.
tftp	Copies the current running configuration or newly stored dynamic voice configuration file to the specified Trivial File Transfer Protocol (TFTP) server. After **copy running-config tftp** or **copy running-config dynvoice-config tftp** is entered, the following prompts require additional information: *Address of remote host:* Specifies the IP address of the TFTP server. *Destination filename:* Specifies the file name to use when storing the copied file on the TFTP server. The file will be placed in the default directory established by the TFTP server.
usbdrive0	Copies the current running configuration to the USB flash drive memory.
username <*username*>	Optional. Specifies a user name to use with HTTP or HTTPS authentication.
xmodem	Copies the current running configuration (using the XMODEM protocol) to the terminal connected to the console port. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 16.1	Command was expanded to include **HTTP** and **HTTPS**.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include USB flash drive memory.
Release R10.5.0	Command was expanded to include the **port**, **username**, and **password** parameters.

Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example copies the current running configuration to the startup configuration file located in flash memory:

>**enable**
#copy running-config flash startup-config
Building configuration...
Done. Success!

The following example copies the current running configuration to CompactFlash memory and names the file **config_01.txt**:

>**enable**
#copy running-config cflash config_01.txt
Percent Compete 100%
#

The following example copies the current running configuration to a TFTP server and names the file **config_01.txt**:

>**enable**
#copy running-config tftp
Address of remote host? **10.200.2.4**
Destination filename? **config_01.txt**
Initiating TFTP transfer...
Sent 3099 bytes.
Transfer Complete!

The following example copies the current running configuration to the connected terminal using XMODEM protocol:

>**enable**
#copy running-config xmodem
Begin the Xmodem transfer now...
Press CTRL+X twice to cancel
CCCCCC

AOS is now ready to transmit the file on the **CONSOLE** port (using the XMODEM protocol). The next step in the process may differ depending on the type of terminal emulation software you are using. For HyperTerminal, you will now select **Transfer > Receive File** and select the destination. Once the transfer is complete, information similar to the following is displayed:

Sent 3704 bytes.
Transfer complete!

copy scp

Use the **copy scp** command to securely copy a file using Secure Copy Protocol (SCP) from a secure shell (SSH) server. Variations of this command include:

copy scp <*url*> **flash** <*filename*>
copy scp <*url*> **flash** <*filename*> **force-overwrite**
copy scp <*url*> **flash** <*filename*> **force-overwrite myprivkey**
copy scp <*url*> **flash** <*filename*> **force-overwrite myprivkey dsa**
copy scp <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa**
copy scp <*url*> **flash** <*filename*> **force-overwrite password** <*password*>
copy scp <*url*> **flash** <*filename*> **force-overwrite port** <*port*>
copy scp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey**
copy scp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey dsa**
copy scp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa**
copy scp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **password** <*password*>
copy scp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **privkey** <*filename*>
copy scp <*url*> **flash** <*filename*> **force-overwrite privkey** <*filename*>
copy scp <*url*> **flash** <*filename*> **myprivkey** <*SSH Authentication key*>
copy scp <*url*> **flash** <*filename*> **myprivkey dsa**
copy scp <url> **flash** <*filename*> **myprivkey ecdsa256**
copy scp <url> **flash** <*filename*> **myprivkey ecdsa384**
copy scp <url> **flash** <*filename*> **myprivkey ecdsa521**
copy scp <*url*> **flash** <*filename*> **myprivkey rsa**
copy scp <*url*> **flash** <*filename*> **myprivkey rsa-sha2-512**
copy scp <url> **flash** <*filename*> **privkey** <*filename*>
copy scp <*url*> **flash** <*filename*> **password** <*password*>
copy scp <*url*> **flash** <*filename*> **port** <*port*>

copy scp <*url*>:<path> **flash** <*filename*> **myprivkey ecdsa256**
copy scp <*url*>:<path>**f lash** <*filename*> **myprivkey ecdsa384**
copy scp <*url*>:<path> **flash** <*filename*> **myprivkey ecdsa521**
copy scp <*url*>:<path> **flash** <*filename*> **myprivkey rsa**
copy scp <*url*>:<path>**f lash** <*filename*> **myprivkey rsa-sha2-512**
copy scp <*url*>:<path> **flash** <*filename*> **privkey** <*filename*>
copy scp <*url*>:<path> **password** <*password*>
copy scp <*url*>:<path> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa256**
copy scp <*url*>:<path> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa384**
copy scp <*url*>:<path> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa521**
copy scp <*url*>:<path> **flash** <*filename*> **port** <*port*> **myprivkey rsa**
copy scp <*url*>:<path> **flash** <*filename*> **port** <*port*> **myprivkey rsa-sha2-512**
copy scp <*url*>:<path> **flash** <*filename*> **port** <*port*> **password**

copy scp <*url*>:<path> flash <filename>

The following variations of this command are valid only on AOS units with CompactFlash® capability:

copy scp <*url*> **cflash** <*filename*> **force-overwrite myprivkey dsa**
copy scp <*url*> **cflash** <*filename*> **force-overwrite myprivkey rsa**
copy scp <*url*> **cflash** <*filename*> **force-overwrite port** <*port*> **myprivkey dsa**
copy scp <*url*> **cflash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa**
copy scp <*url*> **cflash** <*filename*> **myprivkey dsa**
copy scp <*url*> **cflash** <*filename*> **myprivkey rsa**
copy scp <*url*> **cflash** <*filename*> **port** <*port*> **myprivkey dsa**
copy scp <*url*> **cflash** <*filename*> **port** <*port*> **privkey rsa**

Syntax Description

<*url*>	Specifies the source uniform resource locator (URL) on the remote server from which the file is copied. Specify the URL in the following format: **user@server: /path/filename**.
cflash	Specifies the file is copied securely to the CompactFlash card.
flash	Specifies the file is copied securely to the flash drive.
<*filename*>	Specifies the name of the file to copy from the SSH server.
force-overwrite	Optional. Specifies the copied file overwrites an existing file.
myprivkey	Optional. Specifies the AOS unit's private key is used for SSH authentication.
dsa	Optional. Specifies to use the unit's Digital Signature Algorithm (DSA) private key for SSH authentication.
rsa	Optional. Specifies to use the unit's Rivest-Shamir-Adleman (RSA) private key for SSH authentication.
password <*password*>	Optional. Specifies a password is used for SSH authentication.
port <*port*>	Optional. Specifies a port to use for the file transfer. Valid range is **1** to **65535**.
privkey <*filename*>	Optional. Specifies a private key is used for SSH authentication. The file name is the name of the private key file in privacy enhanced email (PEM) format.

Default Values

No default values are necessary for this command.

Command History

Release R14.4.0	Command was expanded to include <url>:<path>.

Usage Examples

The following example uses SCP to copy **FILE1** securely to flash from the SSH server **john@server1.** SSH authentication is performed using a password:

>**enable**
#copy scp john@server1:/FILE1 flash FILE1 password PSWD

copy sftp

Use the **copy sftp** command to securely copy a file using Secure File Transfer Protocol (SFTP) from a secure shell (SSH) server. Variations of this command include:

copy sftp <*url*> **flash** <*filename*>
copy sftp <*url*> **flash** <*filename*> **force-overwrite**
copy sftp <*url*> **flash** <*filename*> **force-overwrite myprivkey**
copy sftp <*url*> **flash** <*filename*> **force-overwrite myprivkey dsa**
copy sftp <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa-sha2-512**
copy sftp <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa-ecdsa256**
copy sftp <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa-ecdsa384**
copy sftp <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa-ecdsa521**
copy sftp <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa**
copy sftp <*url*> **flash** <*filename*> **force-overwrite privkey** <*filename*>
copy sftp <*url*> **flash** <*filename*> **force-overwrite password** <*password*>
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*>
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey**
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey dsa**
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa-sha2-512**
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa256**
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa384**
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa521**
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa**
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **password** <*password*>
copy sftp <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **privkey** <*filename*>
copy sftp <*url*> **flash** <*filename*> **myprivkey** <*SSH Authentication key*>
copy sftp <*url*> **flash** <*filename*> **myprivkey dsa**
copy sftp <url> **flash** <*filename*> **myprivkey ecdsa256**
copy sftp <url> **flash** <*filename*> **myprivkey ecdsa384**
copy sftp <url> **flash** <*filename*> **myprivkey ecdsa521**
copy sftp <*url*> **flash** <*filename*> **myprivkey rsa**
copy sftp <*url*> **flash** <*filename*> **myprivkey rsa-sha2-512**
copy sftp <url> **flash** <*filename*> **privkey** <*filename*>
copy sftp <*url*> **flash** <*filename*> **password** <*password*>
copy sftp <*url*> **flash** <*filename*> **port** <*port*>

Syntax Description

<*url*>	Specifies the source uniform resource locator (URL) on the remote server from which the file is copied. Specify the URL in the following format: **user@server: /path/filename**.
flash	Specifies the file is copied securely to the flash drive.
<*filename*>	Specifies the name of the file to copy from the SSH server.

force-overwrite	Optional. Specifies the copied file overwrites an existing file.
myprivkey	Optional. Specifies the AOS unit's private key is used for SSH authentication.
dsa	Optional. Specifies to use the unit's Digital Signature Algorithm (DSA) private key for SSH authentication.
rsa	Optional. Specifies to use the unit's Rivest-Shamir-Adleman (RSA) private key for SSH authentication.
ecdsa	Optional. Specifies to use unit's ECDSAnistp256|384|521 private keys for SSH authentication.
password <*password*>	Optional. Specifies a password is used for SSH authentication.
port <*port*>	Optional. Specifies a port to use for the file transfer. Valid range is **1** to **65535**.
privkey <*filename*>	Optional. Specifies a 3rd party private key is used for SSH authentication. The file name is the name of the private key file in privacy enhanced email (PEM) format.

Default Values

No default values are necessary for this command.

Command History

Release R13.11.0	Command was introduced.

Usage Examples

The following example uses SFTP to copy **FILE1** securely to flash from the SSH server **john@server1.** SSH authentication is performed using a password:

>**enable**
#copy sftp john@server1:/FILE1 flash FILE1 password PSWD

copy vrf

Use the **copy vrf** command to securely copy a file from a virtual routing and forwarding (VRF) instance. Variations of this command include:

copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **myprivkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **myprivkey dsa**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **myprivkey ecdsa256**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **myprivkey ecdsa384**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **myprivkey ecdsa521**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **myprivkey rsa**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **privkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **password**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **myprivkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **myprivkey** dsa
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **myprivkey ecdsa256**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **myprivkey ecdsa384**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **myprivkey ecdsa521**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **myprivkey rsa**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **privkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **scp** <*url*> **port** <*port*> **password**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **myprivkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **myprivkey dsa**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **myprivkey ecdsa256**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **myprivkey ecdsa384**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **myprivkey ecdsa521**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **myprivkey rsa**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **privkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **password**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **myprivkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **myprivkey** dsa
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **myprivkey ecdsa256**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **myprivkey ecdsa384**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **myprivkey ecdsa521**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **myprivkey rsa**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **privkey** <*filename*>
copy vrf <*name*> **flash** <*filename*> **sftp** <*url*> **port** <*port*> **password**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **myprivkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **myprivkey dsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **myprivkey ecdsa256**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **myprivkey ecdsa384**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **myprivkey ecdsa521**

copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **myprivkey rsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **privkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **password**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey dsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa256**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa384**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa521**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey rsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **privkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **port** <*port*> **password**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey dsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey ecdsa256**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey ecdsa384**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey ecdsa521**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa-sha2-512**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite privkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite password**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey dsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa256**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa384**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa521**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **privkey** <*filename*>
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **password**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **myprivkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **myprivkey dsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **myprivkey ecdsa256**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **myprivkey ecdsa384**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **myprivkey ecdsa521**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **myprivkey rsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **privkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **password**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey dsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa256**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa384**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey ecdsa521**

copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey rsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **privkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **port** <*port*> **password**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite myprivkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite myprivkey dsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite myprivkey ecdsa256**
copy vrf <*name*> **sftp** <*url*> **flash** <*filename*> **force-overwrite myprivkey ecdsa384**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite myprivkey ecdsa521**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite myprivkey rsa-sha2-512**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite privkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite password**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey dsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa256**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa384**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey ecdsa521**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **myprivkey rsa-sha2-512**
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **privkey** <*filename*>
copy vrf <*name*> **scp** <*url*> **flash** <*filename*> **force-overwrite port** <*port*> **password**

Syntax Description

<*filename*>	Specifies the name of the file to copy.
flash	Specifies the file is copied securely to the flash drive.
force-overwrite	Optional. Specifies the copied file overwrites an existing file.
myprivkey	Optional. Specifies the AOS unit's private key is used for SSH authentication.
dsa	Optional. Specifies to use the unit's Digital Signature Algorithm (DSA) private key for SSH authentication.
rsa	Optional. Specifies to use the unit's Rivest-Shamir-Adleman (RSA) private key for SSH authentication.
ecdsa	Optional. Specifies to use the unit's Rivest-Shamir-Adleman (RSA) private key for SSH authentication.
password <*password*>	Optional. Specifies a password is used for SSH authentication.
port <*port*>	Optional. Specifies a port to use for the file transfer. Valid range is **1** to **65535**.

privkey *<filename>*	Optional. Specifies a private key is used for SSH authentication. The file name is the name of the private key file in privacy enhanced email (PEM) format.
scp *<url>*	Specifies the Secure Copy Protocol (SCP) server Uniform Resource Locator (URL) to which to transfer the source file. Specify the URL in the following format: **user@server:/path/filename.**
sftp *<url>*	Specifies the Secure File Transfer Protocol server Uniform Resource Locator (URL) to which to transfer the source file. Specify the URL in the following format: **user@server:/path/filename.**
vrf *<name>*	Specifies a non-default virtual routing and forwarding (VRF) instance from which to copy the file.
flash	Specifies the file is copied securely from the flash drive.
scp *<url>*	Specifies the Secure Copy Protocol (SCP) server Uniform Resource Locator (URL) from which to transfer the source file. Specify the URL in the following format: **user@server:/path/filename.**
sftp *<url>*	Specifies the Secure File Transfer Protocol server Uniform Resource Locator (URL) from which to transfer the source file. Specify the URL in the following format: **user@server:/path/filename.**

Default Values

No default values are necessary for this command.

Command History

Release R10.10	Command was introduced.
Release R13.11.	Command was expanded to include **sftp**, **myprivkey**, **myprivkey dsa** and **myprivkey rsa**.
Release 14.4.0	Command was expanded to include **myprivkey ecdsa** for **sftp** and **scp** options.

Usage Examples

The following example uses SCP to copy **FILE1** from the VRF instance **V1** on the SSH server **john@server1** and performs SSH authentication using a password:

>**enable**
#copy vrf V1 scp john@server1:/FILE1 flash FILE1 password PSWD <filename>
#copy scp V1scp john@server1:/FILE1 flash FILE1 password PSWD <filename>

copy startup-config

Use the **copy startup-config** command to create a copy of the current startup configuration file and replace the current running configuration or save it to a specified memory location.

Variations of this command (valid on all AOS units) include:

copy startup-config *<filename>*
copy startup-config http *<url>*
copy startup-config http *<url>* **username** *<username>* **password** *<password>*
copy startup-config http *<url>* **port** *<port>*
copy startup-config http *<url>* **port** *<port>* **username** *<username>* **password** *<password>*
copy startup-config https *<url>*
copy startup-config https *<url>* **allow-tls1.0**
copy startup-config https *<url>* **allow-tls1.0 allow-tls1.1**
copy startup-config https *<url>* **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy startup-config https *<url>* **allow-tls1.0 allow-sslv3**
copy startup-config https *<url>* **allow-tls1.1**
copy startup-config https *<url>* **allow-tls1.1 allow-sslv3**
copy startup-config https *<url>* **allow-sslv3**
copy startup-config https *<url>* **username** *<username>* **password** *<password>*
copy startup-config https *<url>* **allow-tls1.0 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **allow-tls1.0 allow-tls1.1 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **allow-tls1.0 allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **allow-tls1.0 allow-sslv3 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **allow-tls1.1 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **allow-sslv3 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **port** *<port>*
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0**
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0 allow-tls1.1**
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3**
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0 allow-sslv3**
copy startup-config https *<url>* **port** *<port>* **allow-sslv3**
copy startup-config https *<url>* **port** *<port>* **username** *<username>* **password** *<password>*
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0 allow-tls1.1 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0 allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **port** *<port>* **allow-tls1.0 allow-sslv3 username** *<username>* **password** *<password>*

copy startup-config https *<url>* **port** *<port>* **allow-tls1.1 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **port** *<port>* **allow-tls1.1 allow-sslv3 username** *<username>* **password** *<password>*
copy startup-config https *<url>* **port** *<port>* **allow-sslv3 username** *<username>* **password** *<password>*
copy startup-config running-config
copy startup-config tftp
copy startup-config xmodem

Variations of this command (valid only on AOS units with CompactFlash® capability) include:

copy startup-config cflash *<filename>*
copy startup-config flash *<filename>*

Variations of this command (valid only on AOS units with **ramdisk** enabled) include:

copy startup-config ramdisk *<filename>*

Variations of this command (valid only on AOS units with Universal Serial Bus (USB) flash drive capability) include:

copy startup-config usbdrive0 *<filename>*

Syntax Description

<filename>	Specifies the file name to use when saving the startup configuration file.
cflash	Copies the startup configuration file and saves it to the CompactFlash card using the specified file name.
flash	Copies the startup configuration file and saves it to flash memory using the specified file name.
http *<url>*	Copies the startup configuration file and transfers it to a Hypertext Transfer Protocol (HTTP) server using the specified HTTP server uniform resource locator (URL). This function use the HTTP PUT operation.
https *<url>*	Copies the startup configuration file and transfers it to a secure socket Hypertext Transfer Protocol Secure (HTTPS) server using the specified HTTPS server URL. This function use the HTTPS PUT operation.
allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0 when transferring the startup configuration file. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS protocol version 1.1 when transferring the startup configuration file. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3 when transferring the startup configuration file. If SSLv3 is enabled, then TLS version 1.0 is automatically enabled.
password *<password>*	Optional. Specifies a password for HTTP or HTTPS authentication.

port <*port*>	Optional. Specifies the port used to transfer the specified file to an HTTP or HTTPS server. Range is **0** to **65335**.
ramdisk <*filename*>	Copies the current startup configuration file to the volatile RAM disk using the specified file name.
running-config	Merges the current running configuration with the startup configuration file.
tftp	Copies the current startup configuration file to a specified Trivial File Transfer Protocol (TFTP) server. After **copy startup-config tftp** is entered, the following prompts require additional information: *Address of remote host:* Specifies the IP address of the TFTP server. *Destination filename:* Specifies the file name to use when storing the copied file on the TFTP server. The file will be placed in the default directory established by the TFTP server.
usbdrive0	Copies the startup configuration and saves it to the USB flash drive memory using the specified file name.
username <*username*>	Optional. Specifies a user name to use with HTTP or HTTPS authentication.
xmodem	Copies the current startup configuration (using the XMODEM protocol) to the terminal connected to the console port. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 16.1	Command was expanded to include **HTTP** and **HTTPS**.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include USB flash drive memory.
Release R10.5.0	Command was expanded to include the **port**, **username**, and **password** parameters.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example copies the startup configuration file to the current running configuration:

>**enable**
#copy startup-config running-config
Opening and applying file...

*Any changes made to the current running configuration of the AOS unit that have not been saved to the startup configuration file (using the **write** command) will be lost when the **copy startup-config running-config** command is entered.*

The following example copies the startup configuration file (located in flash memory) to CompactFlash and names the file **config_01.txt**:

>**enable**
#copy startup-config cflash config_01.txt
Percent Complete 100%
#

The following example copies the current startup configuration file to a TFTP server and names the file **startup_01.txt**:

>**enable**
#copy startup-config tftp
Address of remote host? **10.200.2.4**
Destination filename? **startup_01.txt**
Initiating TFTP transfer...
Sent 3099 bytes.
Transfer Complete!
The following example copies the current startup configuration to the connected terminal using XMODEM protocol:

>**enable**
#copy startup-config xmodem
Begin the Xmodem transfer now...
Press CTRL+X twice to cancel
CCCCCC

AOS is now ready to transmit the file on the **CONSOLE** port (using the XMODEM protocol). The next step in the process may differ depending on the type of terminal emulation software you are using. For HyperTerminal, you will now select **Transfer > Receive File** and select the destination. Once the transfer is complete, information similar to the following is displayed:

Sent 3704 bytes.
Transfer complete!

copy tftp

Use the **copy tftp** command to copy a file located on a network Trivial File Transfer Protocol (TFTP) server to a specified destination.

Variations of this command (valid on all AOS units) include:

copy tftp flash
copy tftp running-config
copy tftp startup-config

Variations of this command (valid only on AOS units with CompactFlash® capability) include:

copy tftp cflash

Variations of this command (valid only on AOS units with CompactFlash AND voice capability) include:

copy tftp dynvoice-config

Variations of this command (valid only on AOS units with **ramdisk** enabled) include:

copy tftp ramdisk

Variations of this command (valid only on AOS units with Universal Serial Bus (USB) flash drive capability) include:

copy tftp usbdrive0

Syntax Description

cflash	Copies a file from the TFTP server to the CompactFlash card.	
dynvoice-config	Specifies that the file copied from the TFTP server overwrite the dynamic voice configuration file.	
flash	Copies a file from the TFTP server to the flash memory.	
ramdisk	Copies a file from the TFTP server to the volatile RAM disk.	
running-config	Replaces the active running configuration with the file copied from the TFTP server.	
startup-config	Replaces the startup configuration with the file copied from the TFTP server.	
	After entering **copy tftp** and specifying the destination, AOS prompts for the following information:	
	Address of remote host:	Specifies the IP address of the TFTP server.
	Source filename:	Specifies the name of the file to copy from the TFTP server.
	Destination filename:	Specifies the file name to use when storing the copied file. (Valid only for the **copy tftp cflash**, **copy tftp flash**, **copy tftp ramdisk** commands.)
usbdrive0	Copies a file from the TFTP server to the USB flash drive memory.	

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include USB flash drive memory.

Usage Examples

The following example replaces the current running configuration file with **newconfig.txt** from the TFTP server (**10.200.2.4**):

#copy tftp running-config
Address of remote host? **10.200.2.4**
Source filename? **newconfig.txt**
Initiating TFTP transfer...
Received 4562 bytes.
Transfer Complete!
#

The following example copies the file **myfile.biz** from the TFTP server (**10.200.2.4**) and saves it CompactFlash memory (naming the copy **newfile.biz**):

#copy tftp cflash
Address of remote host? **10.200.2.4**
Source filename? **myfile.biz**
Destination filename? **newfile.biz**
Initiating TFTP transfer...
Received 45647 bytes.
Transfer Complete!
#

copy tftp dot11ap

Use the **copy tftp dot11ap** command to upgrade the firmware on a specific access point (AP) using Trivial File Transfer Protocol (TFTP). Variations of this command include:

copy tftp dot11ap interface <*ap number*>
copy tftp dot11ap mac-address <*mac address*>

Syntax Description

interface <*ap number*>	Specifies the AP interface number to which to apply the firmware upgrade.
mac-address <*mac address*>	Specifies the medium access control (MAC) address of the AP's physical Ethernet interface to which to apply the firmware upgrade. Enter MAC addresses in the format **HH:HH:HH:HH:HH:HH**.

Default Values

No default values are necessary for this command.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example specifies that a firmware upgrade is applied using TFTP to the AP interface **2**:

>**enable**
#copy tftp dot11ap interface 2

copy usbdrive0

Use the **copy usbdrive0** command to copy files located in Universal Serial Bus (USB) flash drive memory to a specified destination.

Variations of this command include:

copy usbdrive0 <*source file*> **boot**
copy usbdrive0 <*source file*> **flash**
copy usbdrive0 <*source file*> **flash** <*new file*>
copy usbdrive0 <*source file*> **http** <*url*>
copy usbdrive0 <*source file*> **http** <*url*> **port** <*port*>
copy usbdrive0 <*source file*> **http** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy usbdrive0 <*source file*> **http** <*url*> **username** <*username*> **password** <*password*>
copy usbdrive0 <*source file*> **https** <*url*>
copy usbdrive0 <*source file*> **https** <*url*> **port** <*port*>
copy usbdrive0 <*source file*> **https** <*url*> **port** <*port*> **username** <*username*> **password** <*password*>
copy usbdrive0 <*source file*> **https** <*url*> **username** <*username*> **password** <*password*>
copy usbdrive0 <*source file*> **startup-config**
copy usbdrive0 tftp
copy usbdrive0 <*source file*> **usbdrive0** <*new file*>
copy usbdrive0 xmodem

Syntax Description

<*new file*>	Saves the file using the specified file name.
<*source file*>	Specifies the name of the file to copy.
boot	Copies the specified source file and overwrites the boot read only memory (ROM).
flash	Copies the specified file and saves it to flash memory.
http <*url*>	Copies the specified source file and transfers it to a Hypertext Transfer Protocol (HTTP) server using the specified HTTP server uniform resource locator (URL). This function uses the HTTP PUT operation.
https <*url*>	Copies the specified source file and transfers it to a secure socket Hypertext Transfer Protocol Secure (HTTPS) server using the specified HTTPS server URL. This function uses the HTTPS PUT operation.
iport <*port*>	Optional. Specifies the port used to transfer the specified file to an HTTP or HTTPS server. Range is **0** to **65335**.
password <*password*>	Optional. Specifies a password to use with HTTP or HTTPS authentication.
startup-config	Replaces the startup configuration file with a copy of the specified file.
tftp	Copies any file located in USB flash drive memory to a specified Trivial File Transfer Protocol (TFTP) server. After **copy usbdrive0 tftp** is entered, the following prompts require additional information: *Address of remote host:* Specifies the IP address of the TFTP server.

	Source filename:	Specifies the name of the file (located in USB flash drive memory) to copy to the TFTP server.
	Destination filename:	Specifies the file name to use when storing the copied file on the TFTP server. The file will be placed in the default directory established by the TFTP server.
usbdrive0 <*new file*>	Copies the specified file and saves it to USB flash drive memory.	
username <*username*>	Optional. Specifies a user name to use with HTTP or HTTPS authentication.	
xmodem	Copies any file located in USB flash drive memory (using the XMODEM protocol) to the PC connected to the console port. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal.	
	After **copy flash xmodem** is entered, the following prompts the require additional information:	
	Source filename:	Specifies the name of the file to copy from USB flash drive memory using XMODEM.

Default Values

No default values are necessary for this command.

Command History

Release 18.2	Command was introduced.
Release R10.5.0	Command was expanded to include the **username** and **password** parameters.

Usage Examples

The following example creates a copy of the file **myfile.biz** (located in USB flash drive memory), names the new file **newfile.biz**, and places the new file in flash memory:

>**enable**
#copy usbdrive0 myfile.biz flash newfile.biz

The following example copies the file **myfile.biz** (located in USB flash drive memory) to CompactFlash memory and names the new file **newfile.biz**:

>**enable**
#copy usbdrive0 myfile.biz cflash newfile.biz

The following example copies the file **new_startup_config.txt** (located in USB flash drive memory) to the startup configuration file:

>**enable**
#copy usbdrive0 new_startup_config.txt startup-config

copy xmodem

Use the **copy xmodem** command to copy a file (using the XMODEM protocol) to a specified destination. XMODEM capability is provided in VT100 terminal emulation software, such as HyperTerminal.

Variations of this command (valid only on AOS units with CompactFlash® capability) include:

copy xmodem cflash

Variations of this command (valid only on AOS units with CompactFlash AND voice capability) include:

copy xmodem dynvoice-config

Variations of this command (valid only on AOS units with **ramdisk** enabled) include:

copy xmodem ramdisk

Variations of this command (valid only on AOS units with Universal Serial Bus (USB) flash drive capability) include:

copy xmodem usbdrive0

Variations of this command (valid on all AOS units) include:

copy xmodem flash
copy xmodem running-config
copy xmodem startup-config

Syntax Description

cflash	Copies a file from the terminal connected to the console port and saves it to the CompactFlash card. After entering **copy xmodem cflash**, AOS prompts for the following information: *Destination filename:* Specifies the file name to use when storing the copied file to cflash memory.
dynvoice-config	Specifies that the file copied from the terminal connected to the console port overwrite the dynamic voice configuration file.
flash	Copies a file from the terminal connected to the console port and saves it to flash memory. After entering **copy xmodem flash**, AOS prompts for the following information: *Destination filename:* Specifies the file name to use when storing the copied file to flash memory.
ramdisk	Copies a file from the terminal connected to the console port and saves it to the volatile RAM disk.
running-config	Replaces the active running configuration with a file copied from the terminal connected to the console port.

startup-config	Replaces the startup configuration with a file copied from the terminal connected to the console port.
usbdrive0	Copies a file from the terminal connected to the console port and saves it to the USB flash drive memory.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include USB flash drive memory.

Usage Examples

The following example copies a software file (**myfile.biz**) to flash memory and renames it **newfile.biz**:

#copy xmodem flash
Destination filename? **newfile.biz**
Begin the Xmodem transfer now...
Press CTRL+X twice to cancel
CCCCCC

AOS is now ready to accept the file on the **CONSOLE** port (using the XMODEM protocol). The next step in the process may differ depending on the type of terminal emulation software you are using. For HyperTerminal, you will now select **Transfer > Send File** and browse to the file you wish to copy **myfile.biz**. Once the transfer is complete, information similar to the following is displayed:

Received 531424 bytes.
Transfer complete

debug aaa

Use the **debug aaa** command to activate debug messages associated with authentication from the authentication, authorization, and accounting (AAA) subsystem. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The **debug aaa** events include connection notices, login attempts, and session tracking.

Usage Examples

The following is sample output for this command:

```
>enable
#debug aaa
AAA: New Session on portal 'TELNET 0 (172.22.12.60:4867)'.
AAA: No list mapped to 'TELNET 0'. Using 'default'.
AAA: Attempting authentication (username/password).
AAA: RADIUS authentication failed.
AAA: Authentication failed.
AAA: Closing Session on portal 'TELNET 0 (172.22.12.60:4867)'.
```

debug activchassis

Use the **debug activchassis** command to enable debug messaging for ActivChassis. Variations of this command include:

debug activchassis
debug activchassis election
debug activchassis fan
debug activchassis filesync
debug activchassis linecard
debug activchassis poe
debug activchassis rpc
debug activchassis sfp

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

election	Optional. Specifies that debug messages for ActivChassis election events are enabled.
fan	Optional. Specifies that debug messages for ActivChassis fan events are enabled.
filesync	Optional. Specifies that debug messages for ActivChassis file synchronization events are enabled.
linecard	Optional. Specifies that debug messages for ActivChassis linecard events are enabled.
poe	Optional. Specifies that debug messages for ActivChassis Power over Ethernet (PoE) events are enabled.
rpc	Optional. Specifies that debug messages for ActivChassis remote procedure call (RPC) events are enabled.
sfp	Optional. Specifies that debug messages for ActivChassis small form-factor pluggable (SFP) interface events are enabled.

Default Values

No default values are necessary for this command.

Command History

Release AC1.0	Command was introduced.
Release R10.7.0	Command was expanded to include the **sfp** parameter.

Usage Examples

The following example enables debug messages for the entire ActivChassis:

>**enable**
#debug activchassis

debug arp

Use the **debug arp** command to activate debug messages associated with IP Address Resolution Protocol (ARP) transactions. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example activates debug messages associated with ARP transactions:

```
>enable
#debug arp
```

debug atm events

Use the **debug atm events** command to display events on all asynchronous transfer mode (ATM) ports and all virtual circuits. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates ATM event messages:

```
>enable
#debug atm events
```

debug atm oam

Use the **debug atm oam** command to display operations, administration, and maintenance (OAM) packets for an asynchronous transfer mode (ATM) virtual circuit descriptor (VCD). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug atm oam
debug atm oam <*vcd*>
debug atm oam <*vcd*> **loopback end-to-end**
debug atm oam <*vcd*> **loopback end-to-end** <*LLID*>
debug atm oam <*vcd*> **loopback segment**
debug atm oam <*vcd*> **loopback segment** <*LLID*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*vcd*>	Optional. Shows OAM packets for a specific VCD.
loopback	Optional. Configures an OAM loopback.
end-to-end	Optional. Configures an end-to-end OAM loopback.
segment	Optional. Configures a segment loopback.
<*LLID*>	Optional. Specifies 16 byte OAM loopback location ID (LLID).

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates ATM OAM debug messages for VCD 1:

>**enable**
#debug atm oam 1

debug atm packet

Use the **debug atm packet** command to activate debug messages associated with packets on asynchronous transfer mode (ATM) ports and virtual circuits. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug atm packet
debug atm packet interface atm <*port id*>
debug atm packet interface atm <*port id*> **vcd** <*number*>
debug atm packet vc <*VPI/VCI*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

interface atm <*port id*>	Optional. Activates packet debug messages for a specific ATM port and for all virtual circuits.
vc <*VPI/VCI*>	Optional. Activates packet debug messages for the specified virtual circuit identified by the virtual path identifier and virtual channel identifier (VPI/VCI).
vcd <*number*>	Optional. Activates packet debug messages for the specified virtual circuit descriptors (VCDs).

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates debug ATM packet debug messages on ATM port 1:

>enable
#debug atm packet interface atm 1

debug auto-config

Use the **debug auto-config** command to activate debug messages associated automatic configuration events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with automatic configuration events:

```
>enable
#debug auto-config
```


debug auto-link

Use the **debug auto-link** command to display event messages for the auto-link feature configuration. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.3/A2	Command was introduced.

Usage Examples

The following example activates auto-link debug messages:

```
>enable
#debug auto-link
```

debug bgp

Use the **debug bgp** command to activate debug messages associated with Internet Protocol version 4 (IPv4) Border Gateway Protocol (BGP). Debug messages display general BGP events, such as sent and received message summaries, route processing actions, and results. These messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug bgp
debug bgp events
debug bgp in
debug bgp out
debug bgp keepalives
debug bgp scan
debug bgp scan database
debug bgp scan route-table
debug bgp scan soft-reset
debug bgp updates
debug bgp updates quiet

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

events	Optional. Displays significant BGP events, such as a neighbor state change.
in/out	Optional. Displays the same information as **debug bgp**, but limits messages to the specified direction (in or out).
keepalives	Optional. Displays BGP keepalive packets.
scan	Optional. Displays BGP background scan details.
database	Optional. Limits output to BGP database scan details.
route-table	Optional. Limits output to BGP route table scan details.
soft-reset	Optional. Limits output to BGP soft reset scan details.
updates	Optional. Displays detailed information on BGP updates for all neighbors.
updates quiet	Optional. Displays summary information about BGP neighbor updates. (Note: **updates quiet** displays a one-line summary of what **update** displays in 104 lines.)

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products. In addition, the **scan**, **database**, **route-table**, and **soft-reset** parameters were added.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products.

Functional Notes

If no arguments are given, the **debug bgp** command displays general BGP events, such as sent/received message summaries, route processing actions, and results. Keepalive packets are not debugged with this command.

Usage Examples

The following example enables debug messages on general outbound BGP messages and events:

>**enable**
#debug bgp out
07:42:39: BGP OUT 10.15.240.1[2]: Transmitting msg, type=UPDATE (2), len=142

debug bridge

Use the **debug bridge** command to display messages associated with bridge events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates bridge debug messages:

```
>enable
#debug bridge
```

debug chat-interfaces *<chat interface>*

Use the **debug chat-interfaces** command to activate debug messages associated with chat AT command-driven interfaces. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

<chat interface>	Activates debug messages for the specified chat interface identified by the slot/port.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages for the chat interface 0/1:

```
>enable
#debug chat-interfaces 0/1
```

debug color

Use the **debug color** command to activate color coding of debug messages. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the color coding of debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.

Functional Notes

Color coding is based on the debug source and color choices are not configurable.

Usage Examples

The following example enables color coding of debug messages:

```
>enable
#debug color
```

debug crypto

Use the **debug crypto** command to activate debug messages associated with cryptographic operations. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug crypto ecies
debug crypto ike
debug crypto ike client authentication
debug crypto ike client configuration
debug crypto ike negotiation
debug crypto pki

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

ecies	Activates debug messages during Elliptic Curve Integrated Encryption Scheme (ECIES) operations. This information could be useful for troubleshooting ECIES encryption/decryption issues.
ike	Activates all IKE debug messages.
ike client authentication	Optional. Displays IKE client authentication messages as they occur.
ike client configuration	Optional. Displays mode-config exchanges as they take place over the IKE security association (SA). It is enabled independently from the **debug ike negotiation** messaging.
ike negotiation	Optional. Activates only IKE key management debug messages (e.g., handshaking).
pki	Activates all public key infrastructure (PKI) debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 4.1	Command was introduced.
Release 6.1	Command was expanded to include the **pki** parameter.
Release R10.5.0	Command syntax was changed to remove **debug crypto ipsec**. IPsec now uses the *debug data-call* command for debug messages.
Release R11.10.0	Command was expanded to include the **ecies** parameter.

Usage Examples

The following example activates the IKE debug messages:

>**enable**
#debug crypto ike

debug data-call

Use the **debug data-call** command to activate debug messages associated with data call errors and events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with data call errors and events:

```
>enable
#debug data-call
```

debug demand-routing

Use the **debug demand-routing** command to activate debug messages associated with demand routing errors and events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates demand routing error and event messages:

```
>enable
#debug demand-routing
```


debug desktop-auditing

Use the **debug desktop-auditing** command to enable debug messages for clients connected to the network. The desktop auditing debug messages include the network access protection (NAP) messages sent between clients and the server. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Debug messages can be activated for all clients connected to the network or only for specific clients. Using the **no** form of this command disables debug messaging for desktop auditing clients. Variations of this command include:

debug desktop-auditing
debug desktop-auditing hostname <*hostname*>
debug desktop-auditing interface gigabit-switchport <*slot/port*>
debug desktop-auditing interface switchport <*slot/port*>
debug desktop-auditing interface xgigabit-switchport <*slot/port*>
debug desktop-auditing ip <*ip address*>
debug desktop-auditing mac <*mac address*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

hostname <*hostname*>	Optional. Activates debug messages only for the client with the specified host name.
interface gigabit-switchport <*slot/port*>	Optional. Activates debug messages only for the client using the specified gigabit switchport interface.
interface switchport <*slot/port*>	Optional. Activates debug messages only for the client using the specified switchport interface.
interface xgigabit-switchport <*slot/port*>	Optional. Activates debug messages only for the client using the specified 10 gigabit switchport interface.
ip <*ip address*>	Optional. Activates debug messages only for the client with the specified IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
mac <*mac address*>	Optional. Activates debug messages only for the client with the specified medium access control (MAC) address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release 17.8	Command was introduced.
Release R10.7.0	Command was expanded to include the switchport and 10 gigabit switchport interfaces.

Usage Examples

The following is sample output of the **debug desktop-auditing** command:

```
2009.08.31 14:30:30 DESKTOP_AUDITING.DHCP.giga-swx 0/5 from 00:E0:29:0E:D5:E3 NAP Capable
    client
2009.08.31 14:30:31 DESKTOP_AUDITING.DHCP.giga-swx 0/24 from 00:E0:29:0E:D5:E5 to
    00:E0:29:0E:D5:E3 NAP Capable Server
2009.08.31 14:30:31 DESKTOP_AUDITING.DHCP.giga-swx 0/5 from 00:E0:29:0E:D5:E3 to
    00:E0:29:0E:D5:E5 NAP SoH: Firewall is 3rd-Party, AutoUpdates not downloading or installing
2009.08.31 14:30:31 DESKTOP_AUDITING.DHCP.giga-swx 0/24 from 00:E0:29:0E:D5:E5 to
    00:E0:29:0E:D5:E3 NAP SoHR: OK
```


debug dial-backup

Use the **debug dial-backup** command to activate debug messages associated with dial-backup operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 1.1	Command was introduced.
Release 2.1	Additional debug messages were implemented for dial-backup operation to Adtran's IQ and Express Series products.

Functional Notes

The **debug dial-backup** command activates debug messages to aid in the troubleshooting of dial-backup links.

Usage Examples

The following example activates debug messages for dial-backup operation:

```
>enable
#debug dial-backup
```

debug dialup-interfaces

Use the **debug dialup-interfaces** command to generate debug messages used to aid in troubleshooting problems with all dialup interfaces, such as the modem or the basic rate interface (BRI) cards. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 2.1	Command was introduced.

Functional Notes

When enabled, these messages provide status information on incoming calls, dialing and answering progress, etc. These messages also give information on why certain calls are dropped or rejected. It is beneficial to use this command when troubleshooting dial backup (in addition to the **debug dial-backup** command).

Usage Examples

The following example activates the debug messages for dialup interfaces:

>enable
#debug dialup-interfaces

debug dns

Use the **debug dns** command to activate debug messages associated with domain naming system (DNS) client operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug dns
debug dns client
debug dns list
debug dns proxy
debug dns query-plan
debug dns resolver-queue
debug dns table

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

client	Optional. Activates debug messages associated with DNS client operation.
list	Optional. Activates debug messages associated with DNS address lists.
proxy	Optional. Activates debug messages associated with DNS proxy operation.
query-plan	Optional. Activates debug messages associated with DNS query plan operation.
resolver-queue	Optional. Activates debug messages associated with DNS resolver queue operation.
table	Optional. Activates debug messages associated with DNS table operation.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 3.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products.
Release R11.6.0	Command was expanded to include the **list**, **query-plan**, and **resolver-queue** parameters.

Functional Notes

The IPv4 and IPv6 DNS capability allows for DNS-based host translation (name-to-address).

Usage Examples

The following example activates debug messages associated with DNS client activity:

>**enable**
#debug dns client

debug dot11 all

Use the **debug dot11 all** command to enable all dot11 debugging for the wireless access controller (AC). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example activates all dot11 debug messages on the AC:

```
>enable
#debug dot11 all
```

debug dot11 client

Use the **debug dot11 client** command to enable all dot11 client debugging for the wireless access controller (AC). Debugging can also be limited to clients on a specific access point (AP) interface. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug dot11 client
debug dot11 client interface dot11ap <*ap interface*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

interface dot11ap <*ap interface*>	Optional. Activates debug messages for the specified AP interface. Range is **1** to **8**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example activates debug messages for clients on AP interface 1:

>**enable**
#debug dot11 client interface dot11ap 1
2006.12.23 19:47:04 Dot11 Client: AP(1) Radio(1) VAP(1)Rx associate command from AP for 00:40:96:AB:3B:5E.
2006.12.23 19:48:40 Dot11 Client: AP(1) Radio(1) VAP(1)Rx disassociate command from AP for 00:40:96:AB:3B:5E.

These debug messages were captured as a wireless client associated and then disassociated with the AP.

debug dot11 config-apply

Use the **debug dot11 config-apply** command to enable debug messages for configuration changes applied to the NetVanta 160 Series access point (AP). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables configuration change application debug messages for the NetVanta 160 Series AP:

```
>enable
#debug dot11 config-apply
```

debug dot11 firmware-upgrade

Use the **debug dot11 firmware-upgrade** command to enable debug messages for firmware upgrades applied to the NetVanta 160 Series access point (AP). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug dot11 firmware-upgrade
debug dot11 firmware-upgrade verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

verbose	Optional. Activates detailed debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables firmware upgrade debug messages for the NetVanta 160 Series AP:

```
>enable
#debug dot11 firmware-upgrade
```


debug dot11 packet-events

Use the **debug dot11 packet-events** command to enable debugging for all 802.11 control protocol packet events. Debugging can also be limited to a specified interface. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug dot11 packet-events
debug dot11 packet-events interface <*interface*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

interface <*interface*>	Optional. Activates debug messages for the specified interface. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **debug dot11 packet-events interface ?** for a complete list of valid interfaces.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example activates packet-events debug messages on access point (AP) interface 1:

>enable
#debug dot11 packet-events interface dot11ap 1
#2006.12.23 18:54:25 Dot11 Packet Events: Rx Echo Req from MAC(00:A0:C8:1D:F8:57) AP(1)
2006.12.23 18:54:25 Dot11 Packet Events: Tx Echo Resp to MAC(00:A0:C8:1D:F8:57) AP(1)
2006.12.23 18:54:29 Dot11 Packet Events: Tx Query Req to MAC(00:A0:C8:1D:F8:57) AP(1)
2006.12.23 18:54:29 Dot11 Packet Events: Rx Query Resp from MAC(00:A0:C8:1D:F8:57) AP(1)
2006.12.23 18:54:36 Dot11 Packet Events: Rx Disc Resp from MAC(00:A0:C8:1D:F8:57) AP(1)

debug dot11 session

Use the **debug dot11 session** command to debug all dot11 sessions for the wireless access controller (AC). Debugging may also be limited to a specified interface. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug dot11 session
debug dot11 session interface <*interface*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

interface <*interface*>	Optional. Activates debug messages for the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **debug dot11 session interface ?** for a complete list of valid interfaces.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example activates all dot11 session debug messages:

>enable
#debug dot11 session
2006.12.23 19:56:22 DOT11.Session : AP 1: AP reboot.
2006.12.23 19:56:22 DOT11.Session : AP 1: Control session lost.
2006.12.23 19:56:22 DOT11.Session : AP 1: Control session established.

debug dynamic-dns

Use the **debug dynamic-dns** command to activate debug messages associated with dynamic domain naming system (DNS). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug dynamic-dns
debug dynamic-dns verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

verbose	Optional. Activates detailed debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates dynamic DNS debug messages:

>enable
#debug dynamic-dns verbose

debug efm bonding

Use the **debug efm bonding** command to enable debug messaging for bonding negotiation links on all Ethernet in the first mile (EFM) groups. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.4.0	Command was introduced.

Usage Examples

The following example enables debug messaging for bonding negotiations an all EFM groups:

```
>enable
#debug efm bonding
```

debug efm config

Use the **debug efm config** command to enable debug messaging for all Ethernet in the first mile (EFM) components configured on the unit. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release A4.05	Command was introduced.

Usage Examples

The following example enables debug messaging for all EFM components:

```
>enable
#debug efm config
```

debug efm oam

Use the **debug efm oam** command to enable debug messaging for all Ethernet in the first mile (EFM) operations, administration, and management (OAM) and pre-provisioning components configured on the unit. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release A4.05	Command was introduced.

Usage Examples

The following example enables debug messaging for all EFM OAM components:

```
>enable
#debug efm oam
```


debug esmc-packets

Use the **debug esmc-packets** command to display raw Ethernet synchronization message channel (ESMC) packet dumps.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example enables the display of raw ESMC packet dumps:

```
>enable
#debug esmc-packets
```

debug ethernet cfm

Use the **debug ethernet cfm** command to activate all debug messages associated with Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Use this command with caution as it causes a large amount of debug information. Large amounts of debug information can adversely affect the performance of your unit. To avoid an excess of debug information generation, select a debug command that does not activate all CFM debug messages at once.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example activates system-wide Ethernet OAM CFM debug messages:

```
>enable
#debug ethernet cfm
2008.09.22 11:00:08 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:00:09 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=195)
2008.09.22 11:00:09 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:00:10 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=196)
2008.09.22 11:00:10 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:00:11 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=197)
2008.09.22 11:00:11 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:00:12 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=198)
2008.09.22 11:00:12 CFM.MD MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
```


debug ethernet cfm alarm

Use the **debug ethernet cfm alarm** command to activate debug messages associated with Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) fault alarms. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet cfm alarm
debug ethernet cfm alarm domain <*domain name*>
debug ethernet cfm alarm domain <*domain name*> **association** <*association name*>
debug ethernet cfm alarm domain <*domain name*> **association** <*association name*> **mep** <*mep id*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

domain <*domain name*>	Optional. Specifies that debug output is limited to alarm information for maintenance endpoints (MEPs) of a specific domain.
association <*association name*>	Optional. Specifies that debug output is limited to alarm information for MEPs of a specific association.
mep <*mep id*>	Optional. Specifies that debug output is limited to alarm information for MEPs that match a specific MEP ID. MEP ID range is **1** to **8191**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables all Ethernet OAM CFM alarm debug messages:

>**enable**
#debug ethernet cfm alarm
2008.09.22 11:06:20 CFM.FNG MD:BenchTest|MA:BenchAssoc|MEP:1|FNG|Set state: FNG_DEFECT
2008.09.22 11:06:22 CFM.FNG MD:BenchTest|MA:BenchAssoc|MEP:1|FNG|Set state:
FNG_REPORT_DEFECT
2008.09.22 11:06:22 CFM.FNG MD:BenchTest|MA:BenchAssoc|MEP:1|FNG|Set state:
FNG_DEFECT_REPORTED
2008.09.22 11:06:22 CFM.MD:BenchTest|MA:BenchAssoc|MEP:1| mep signaled new fault

debug ethernet cfm ccm rcv

Use the **debug ethernet cfm ccm rcv** command to activate debug messages associated with Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) continuity check message (CCM) receive paths. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet cfm ccm rcv
debug ethernet cfm ccm rcv domain <*domain name*>
debug ethernet cfm ccm rcv domain <*domain name*> **association** <*association name*>
debug ethernet cfm ccm rcv domain <*domain name*> **association** <*association name*> **mep** <*mep id*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

domain <*domain name*>	Optional. Specifies that debug output is limited to CCM receive path information for maintenance endpoints (MEPs) of a specific domain.
association <*association name*>	Optional. Specifies that debug output is limited to CCM receive path information for MEPs of a specific association.
mep <*mep id*>	Optional. Specifies that debug output is limited to CCM receive path information for MEPs that match a specific MEP ID. MEP ID range is **1** to **8191**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables Ethernet OAM CFM debug messages for all CCM receive paths:

>**enable**
#debug ethernet cfm ccm rcv
2008.09.22 11:02:49 CFM.CCR MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:02:50 CFM.CCR MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:02:51 CFM.CCR MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:02:52 CFM.CCR MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2
2008.09.22 11:02:53 CFM.CCR MD:BenchTest|MA:BenchAssoc|MEP:1|CCR|Rx CCM from MEPID 2

debug ethernet cfm ccm xmit

Use the **debug ethernet cfm ccm xmit** command to activate debug messages associated with Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) continuity check message (CCM) transmit paths. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet cfm ccm xmit
debug ethernet cfm ccm xmit domain <*domain name*>
debug ethernet cfm ccm xmit domain <*domain name*> **association** <*association name*>
debug ethernet cfm ccm xmit domain <*domain name*> **association** <*association name*> **mep** <*mep id*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

domain <*domain name*>	Optional. Specifies that debug output is limited to CCM transmit path information for maintenance endpoints (MEPs) of a specific domain.
association <*association name*>	Optional. Specifies that debug output is limited to CCM transmit path information for MEPs of a specific association.
mep <*mep id*>	Optional. Specifies that debug output is limited to CCM transmit path information for MEPs that match a specific MEP ID. MEP ID range is **1** to **8191**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables Ethernet OAM CFM debug messages for all CCM transmit paths:

>**enable**
#debug ethernet cfm ccm xmit
2008.09.22 11:01:43 CFM.CCM MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=290)
2008.09.22 11:01:44 CFM.CCM MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=291)
2008.09.22 11:01:45 CFM.CCM MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=292)
2008.09.22 11:01:46 CFM.CCM MD:BenchTest|MA:BenchAssoc|MEP:1|CCM|Sent CCM (ID=293)

debug ethernet cfm linktrace

Use the **debug ethernet cfm linktrace** command to activate debug messages associated with Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) linktrace message paths. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet cfm linktrace request
debug ethernet cfm linktrace request domain <*domain name*>
debug ethernet cfm linktrace request domain <*domain name*> **association** <*association name*>
debug ethernet cfm linktrace request domain <*domain name*> **association** <*association name*> **mep** <*mep id*>
debug ethernet cfm linktrace response
debug ethernet cfm linktrace response domain <*domain name*>
debug ethernet cfm linktrace response domain <*domain name*> **association** <*association name*>
debug ethernet cfm linktrace response domain <*domain name*> **association** <*association name*> **mep** <*mep id*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

request	Specifies debug messages are enabled for linktrace message request paths.
response	Specifies debug messages are enabled for linktrace message response paths.
domain <*domain name*>	Optional. Specifies that debug output is limited to linktrace message path information for maintenance endpoints (MEPs) of a specific domain.
association <*association name*>	Optional. Specifies that debug output is limited to linktrace message path information for MEPs of a specific association.
mep <*mep id*>	Optional. Specifies that debug output is limited to linktrace message path information for MEPs that match a specific MEP ID. MEP ID range is **1** to **8191**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables Ethernet OAM CFM debug messages for all linktrace message request paths:

```
>enable
#debug ethernet cfm linktrace request
```


debug ethernet cfm loopback

Use the **debug ethernet cfm loopback** command to activate debug messages associated with Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) loopback message paths. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet cfm loopback request
debug ethernet cfm loopback request domain <*domain name*>
debug ethernet cfm loopback request domain <*domain name*> **association** <*association name*>
debug ethernet cfm loopback request domain <*domain name*> **association** <*association name*> **mep** <*mep id*>
debug ethernet cfm loopback response
debug ethernet cfm loopback response domain <*domain name*>
debug ethernet cfm loopback response domain <*domain name*> **association** <*association name*>
debug ethernet cfm loopback response domain <*domain name*> **association** <*association name*> **mep** <*mep id*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

request	Specifies debug messages are enabled for loopback message request paths.
response	Specifies debug messages are enabled for loopback message response paths.
domain <*domain name*>	Optional. Specifies that debug output is limited to loopback message path information for maintenance endpoints (MEPs) of a specific domain.
association <*association name*>	Optional. Specifies that debug output is limited to loopback message path information for MEPs of a specific association.
mep <*mep id*>	Optional. Specifies that debug output is limited to loopback message path information for MEPs that match a specific MEP ID. MEP ID range is **1** to **8191**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables Ethernet OAM CFM debug messages for all loopback message request paths:

```
>enable
#debug ethernet cfm loopback request
```


debug ethernet cfm remote-mep

Use the **debug ethernet cfm remote-mep** command to activate debug messages associated with Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) remote maintenance endpoints (MEPs). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet cfm remote-mep
debug ethernet cfm remote-mep domain <*domain name*>
debug ethernet cfm remote-mep domain <*domain name*> **association** <*association name*>
debug ethernet cfm remote-mep domain <*domain name*> **association** <*association name*>
mep <*mep id*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

domain <*domain name*>	Optional. Specifies that debug output is limited to information for remote maintenance endpoints (MEPs) of a specific domain.
association <*association name*>	Optional. Specifies that debug output is limited to information for remote MEPs of a specific association.
mep <*mep id*>	Optional. Specifies that debug output is limited to information for remote MEPs that match a specific MEP ID. MEP ID range is **1** to **8191**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables Ethernet OAM CFM debug messages for all remote MEPs:

>**enable**
#debug ethernet cfm remote-mep
2008.09.22 11:13:50 CFM.RMEP MD:BenchTest|MA:BenchAssoc|MEP:1|RMEP|Set CCMdefect: true
2008.09.22 11:13:53 CFM.MD:BenchTest|MA:BenchAssoc|MEP:1| mep signaled new fault alarm state (3)

debug ethernet lmi interface <*interface*>

Use the **debug ethernet lmi** command to enable debug messages of Ethernet local management interface (E-LMI) events or packets. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet lmi interface <*interface*> **event**
debug ethernet lmi interface <*interface*> **packet**

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

interface <*interface*>	Specifies an interface on which to enable E-LMI debug messages. Specify interfaces in the format <*interface type [slot/port]*>. For example, for a Gigabit Ethernet interface, use **gigabit eth 0/1**. Type **debug ethernet lmi interface ?** for a complete list of interfaces.
event	Specifies that debug messages for E-LMI events are generated.
packet	Specifies that debug messages for E-LMI packets are generated.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example enables debug messages for E-LMI events on the Gigabit Ethernet interface:

>enable
#debug ethernet lmi interface gigabit-ethernet 0/1 event

debug ethernet oam

Use the **debug ethernet oam** command to activate all debug messages associated with Ethernet Link operations, administration, and maintenance (OAM) configurations. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ethernet oam interface <*interface*>
debug ethernet oam interface <*interface*> **critical**
debug ethernet oam interface <*interface*> **discovery**
debug ethernet oam interface <*interface*> **link-monitor**
debug ethernet oam interface <*interface*> **packet**

Turning on a large amount of debug information can adversely affect the performance of your unit

Syntax Description

interface <*interface*>	Enables Ethernet Link OAM debug messaging on the interface, and specifies that debug output for all Ethernet Link OAM configurations, except OAM PDU transmissions, are included in the debug output. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for a Gigabit Ethernet interface, use **giga-eth 0/1**. For an Ethernet in the first mile (EFM) group, use **efm-group 1/1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.
critical	Optional. Specifies that debug output is limited to link event messages for the specified interface.
discovery	Optional. Specifies that debug output is limited to Ethernet Link OAM discovery processes on the specified interface.
link-monitor	Optional. Specifies that debug output is limited to link event message processing on the specified interface.
packet	Optional. Specifies that debug output is limited to information for transmitted and received OAM PDUs on the specified interface.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables debug messaging for Ethernet Link OAM link monitoring events on the Gigabit Ethernet **0/1** interface:

>**enable**
#debug ethernet oam gigabit-ethernet 0/1 link-monitor
2013.08.28 18:10:11 LINK_OAM.giga-eth 0/1 link-monitor
Processing Link Event Notification PDU, sequence number: 3
    Type: Errored Frame
        Timestamp: 0
        Window: 10
        Threshold: 1
        Errored Frames: 16
        Error Running Total: 0
        Event Running Total: 3

2013.08.28 18:10:12 LINK_OAM.giga-eth 0/2 link-monitor
Processing Link Event Notification PDU, sequence number: 4
    Type: Errored Frame
        Timestamp: 0
        Window: 10
        Threshold: 1
        Errored Frames: 16
        Error Running Total: 0
        Event Running Total: 4

debug frame-relay lmi

Use the **debug frame-relay lmi** command to activate debug messages associated with the Frame Relay operation for the local management interface (LMI), such as data link connection identifier (DLCI) status signaling state, etc. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 1.1	Command was introduced.
Release 17.6	Command was altered to remove **events** and **llc2** options.

Functional Notes

The **debug frame-relay lmi** command activates debug messages to aid in the troubleshooting of Frame Relay links.

Usage Examples

The following example activates debug messages associated with Frame Relay LMI operation:

```
>enable
#debug frame-relay lmi
```


debug frame-relay multilink

Use the **debug frame-relay multilink** command to activate debug messages associated with Frame Relay multilink operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug frame-relay multilink
debug frame-relay multilink <*interface*>
debug frame-relay multilink states

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*interface*>	Optional. Activates debug messages for the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **debug frame-relay multilink ?** for a complete list of applicable interfaces.
states	Optional. Activates the debug messages for Link Integrity Protocol (LIP).

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with multilink operation for all Frame Relay interfaces:

>**enable**
#debug frame-relay multilink

debug global-policer

Use the **debug global-policer** command to activate debug messages associated with the virtual AOS (vAOS) global policer. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R12.1.0	Command was introduced.

Functional Notes

The **debug global-policer** events include expiration of warning event periods or installation of new vAOS licenses.

Usage Examples

The following is sample output for this command when a warning event period has expired:

```
>enable
#debug global-policer
2016.06.20 16:23:27 GLOBAL_POLICER Warning event period expired
    Time since most recent interface statistics clear: never
    Output bytes: 5338483 previous, 5347457 current
    Dropped packets: 0 previous, 0 current
    Dropped bytes: 0 previous, 0 current
2016.06.20 16:23:27 GLOBAL_POLICER Average rate last interval = 239 bps; threshold = 45000000 bps
```

The following is sample output for this command when a new vAOS license is installed:

```
>enable
#debug global-policer
2016.06.20 18:22:00 GLOBAL_POLICER Updated CIR = 50 Mbps; CBS = 5625000 bytes
```


debug gvrp bpdus

Use the **debug gvrp bpdus** command to display debug messages showing all GARP VLAN Registration Protocol (GVRP) configuration messages sent and received on the switch. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Functional Notes

With GVRP enabled on many ports, this command can produce a lot of output. To display these messages for individual interfaces, refer to the command *debug gvrp interface <interface> on page 340*.

Usage Examples

The following example displays debug messages showing GVRP configuration messages sent and received on Ethernet interface 0/24:

```
>enable
#debug gvrp bpdus
2000.07.31 23:15:51 GVRP BPDUS.eth 0/24: TX = (Len:2 LeaveAll) (Len:4 JoinIn Vlan:1) (End) ... SENT
2000.07.31 23:15:52 GVRP BPDUS.eth 0/24: RX = (Len:4 Empty Vlan:2) (Len:4 JoinIn Vlan:20) (end)
2000.07.31 23:15:52 GVRP BPDUS.eth 0/24: TX = (Len:4 JoinIn Vlan:1) (End) ... SENT
2000.07.31 23:15:52 GVRP BPDUS.eth 0/24: RX = (Len:4 JoinIn Vlan:20) (end)
2000.07.31 23:16:00 GVRP BPDUS.eth 0/24: RX = (Len:2 LeaveAll) (end)
#
```


debug gvrp interface *<interface>*

Use the **debug gvrp interface** command to display GARP VLAN Registration Protocol (GVRP) debug messages related to a particular interface. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug gvrp interface <*interface*> **bpdus**
debug gvrp interface <*interface*> **vlans**

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<interface>	Activates debug messages for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **debug gvrp interface ?** for a complete list of applicable interfaces.
bpdus	Displays debug messages showing all GVRP configuration messages sent and received on the interface.
vlans	Displays debug messages showing all GVRP-related VLAN changes occurring on the interface.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example displays debug messages showing GVRP configuration messages sent and received on Ethernet interface 0/24:

>**enable**
#debug gvrp interface ethernet 0/24 bpdus
2000.07.31 23:15:51 GVRP BPDUS.eth 0/24: TX = (Len:2 LeaveAll) (Len:4 JoinIn Vlan:1) (End) ... SENT
2000.07.31 23:15:52 GVRP BPDUS.eth 0/24: RX = (Len:4 Empty Vlan:2) (Len:4 JoinIn Vlan:20) (end)
2000.07.31 23:15:52 GVRP BPDUS.eth 0/24: TX = (Len:4 JoinIn Vlan:1) (End) ... SENT
--MORE--

debug gvrp vlans

Use the **debug gvrp vlans** command to display debug messages showing all GARP VLAN Registration Protocol (GVRP) VLAN changes. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug gvrp vlans
debug gvrp vlans <*vlan id*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*vlan id*>	Optional. Activates debug messages for GVRP-related VLAN changes for the specified VLAN. Range is **1** to **4094**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Functional Notes

With GVRP enabled on many ports, this command can produce a lot of output. To display these messages for an individual interface, refer to the command *debug gvrp interface <interface> on page 340*.

Usage Examples

The following example displays debug messages showing GVRP-related VLAN changes for VLAN 1:

```
>enable
#debug gvrp vlans 1
#
2000.07.31 22:05:42 GVRP VLANS: Creating dynamic VLAN 20
2000.07.31 22:05:42 GVRP VLANS.eth 0/24: Dynamically adding port to VLAN 20
#
2000.07.31 22:05:56 INTERFACE_STATUS.eth 0/24 changed state to down
2000.07.31 22:06:08 GVRP VLANS.eth 0/24: Dynamically removing port from VLAN 20
2000.07.31 22:06:08 GVRP VLANS: Last port removed from VLAN 20, destroying VLAN
```


debug hmr

Use the **debug hmr** command to enable debug messaging for either Session Initiation Protocol (SIP) header manipulation rules (HMR) processes or rules. Use the **no** form of this command to disable debug messages. Variations of this command include:

debug hmr
debug hmr configuration
debug hmr traffic

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

configuration	Optional. Specifies that whenever HMR configuration changes, debug messages outlining HMR rule configuration events are generated.
traffic	Optional. Specifies that whenever HMR policies are applied to traffic, debug messages outlining HMR message processing events are generated.

Default Values

By default, debug messaging is disabled. When HMR debug messaging is enabled, if neither optional keyword is specified when the command is entered, then HMR debug messages are generated on any HMR rule changes that occur.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example enables debug messaging for HMR policies and their application to SIP traffic:

```
>enable
#debug sip stack messages
#debug hmr traffic
00:52:13.323 SIP.STACK MSG          Rx: UDP src=10.17.142.1:5060 dst=10.17.142.252:5060
00:52:13.323 SIP. STACK MSG                 INVITE sip:2565550052@10.17.142.252 SIP /2.0
00:52:13.324 SIP. STACK MSG                 Via: SIP/2.0/UDP
    10.17.142.1:5060;branch=z9hG4bk-2834-1-0
00:52:13.324 SIP. STACK MSG                 From: 2565550052
    <sip:256555052@10.17.142.1:5060;tag=2384SIPpTag001>
00:52:13.325 SIP. STACK MSG                 To: 2565550051
    <sip:2565550051@10.17.142.252:5060>
00:52:13.325 SIP. STACK MSG                 Call-ID: 1-2384@10.17.142.1
00:52:13.326 SIP.STACK MSG
```



```
    CSeq: 1 INVITE
00:52:13.327 SIP.STACK MSG
    Contact: 2565550052 <sip:2565550052@10.17.142.1:5060;transport=UDP>
00:52:13.327 SIP.STACK MSG
    Max-forwards: 70
00:52:13.328 SIP.STACK MSG
    Content-Type: application/sdp
00:52:13.328 SIP.STACK MSG
    Content-Length: 132
00:52:13.329 SIP.STACK MSG
00:52:13.329 SIP.STACK MSG
    v=0
00:52:13.329 SIP.STACK MSG
    o=user1 53655765 2353687637 IN IP4 10.17.142.1
00:52:13.330 SIP.STACK MSG
    s=-
00:52:13.330 SIP.STACK MSG
    c=IN IP4 10.17.142.1
00:52:13.331 SIP.STACK MSG
    t=0 0
00:52:13.332 SIP.STACK MSG
    m=audio 10000 RTP/AVP 0
00:52:13.332 SIP.STACK MSG
    a-rtpmap:0 PCMU/8000
00:52:13.332 SIP.STACK MSG
00:52:13.337 SIP.HMR PROCESS
    Processing SIP message with compiled policy myPolicy
00:52:13.337 SIP.HMR PROCESS
    Rule matches message, applying action rules
00:52:13.338 SIP.HMR PROCESS
    Modifying SIP message headers matching from
00:52:13.338 SIP.HMR PROCESS
    Header From: changed to 2565550052 <sip:2565550052@10.17.142.1:5060>;tag=2384SIPpTag001
00:52:13.339 SIP.HMR PROCESS
    Found 1 headers: Modified 1 headers using /(.*)(;tag.*)/
```

debug http client

Use the **debug http client** command to activate debug messages associated with Hypertext Transfer Protocol (HTTP) client operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products.

Usage Examples

The following example activates debug messages associated with HTTP client activity:

```
>enable
#debug http client
```


debug http server

Use the **debug http server** command to activate debug messages associated with Hypertext Transfer Protocol (HTTP) server operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug http server
debug http server verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

verbose	Optional. Activates detailed debug messages for HTTP operation.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 6.1	Command was introduced.
Release 15.1	Command was updated.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products.

Usage Examples

The following example activates debug messages associated with HTTP server activity:

>enable
#debug http server

debug hw-access-list <*name*>

Use the **debug hw-access-list** command to activate debug messages that display traffic matches logged by the named hardware access control list (ACL). Use the **no** form of this command to disable the debug messages.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

<*name*>	Specifies the name of the hardware ACL.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.6	Command was introduced.

Functional Notes

The **debug hw-access-list** <*name*> command displays data gathered by a configured hardware ACL. The specified hardware ACL must have logging enabled to populate the debug message. For more information on hardware ACLs and event match logging, refer to the *Hardware ACL and Access Map Command Set on page 4235*.

> NOTE *Only hardware ACL debug messages can be displayed using this command. If you enter a software ACL name in this command, you will receive an error message.*

Usage Examples

Enter the command as follows to enable debug messages for the hardware ACL **ADTN**:

```
>enable
#debug hw-access-list ADTN
2009.05.07 11:32:39 ACCESS_LIST.ADTN   permit mac 00:a0:c8:00:00:00 00:00:00:ff:ff:ff any log
    (44864 matches)

2009.05.07 11:32:45 ACCESS_LIST.ADTN   permit mac 00:a0:c8:00:00:00 00:00:00:ff:ff:ff any log
    (106 matches)

2009.05.07 11:32:49 ACCESS_LIST.ADTN   permit mac 00:a0:c8:00:00:00 00:00:00:ff:ff:ff any log
    (90 matches)
```


debug interface <*interface*>

Use the **debug interface** command to activate debug messages associated with the specified interface. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<interface>	Activates debug messages for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **debug interface ?** for a complete list of applicable interfaces.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 3.1	Command was introduced.
Release 6.1	Command was expanded to include the T1 and foreign exchange station (FXS) interfaces.
Release 7.1	Command was expanded to include the foreign exchange office (FXO) interface.
Release 9.1	Command was expanded to include the tunnel interface.
Release A4.05	Command was expanded to include the asymmetric digital subscriber line (ADSL) interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release 13.1.0	Command was expanded to include the virtual extensible local area network (VxLAN) tunnel interface.

Functional Notes

The **debug interface** command activates debug messages to aid in the troubleshooting of physical interfaces.

Usage Examples

The following example activates debug messages associated with tunnel interface 1, which is configured as a (virtual extensible local area network) VxLAN type tunnel:

>**enable**
#debug interface tunnel 1
2017.05.05 05:52:32 TUNNEL.1 VxLAN: Encapsulating original packet 10.0.2.15->10.0.2.17 (len=178 ttl=255).
2017.05.05 05:53:12 TUNNEL.1 Vxlan Rx: Decapsulating original packet 10.0.2.17->10.0.2.15 (len=58 ttl=253 Protocol=17).
2017.05.05 05:53:12 TUNNEL.1 Vxlan Rx: ARP Request/Reply theHardwareType:1, theProtocolType:800, theHardwareSize:4, theProtocolSize:0, theOpcode=1, senderMac:00:11:22:33:44:AB, senderIp:10.10.10.1, vni:200
2017.05.05 05:53:12 TUNNEL.1 Vxlan Rx: PostDecapsulate: VNI=200,
2017.05.05 05:53:12 TUNNEL.1 VxLAN: Encapsulating original packet 10.0.2.15->10.0.2.17 (len=178 ttl=255).
2017.05.05 05:55:59 TUNNEL.1 Vxlan Tx: Packet Size exceeds tunnel MTU. Dropping packet
2017.05.05 05:55:59 TUNNEL.1 VxLAN: Encapsulating original packet 10.0.2.15->10.0.2.17 (len=98 ttl=255).
2017.05.05 05:56:01 TUNNEL.1 Vxlan Tx: Packet Size exceeds tunnel MTU. Dropping packet
2017.05.05 06:01:18 TUNNEL.1 Vxlan Rx: ARP Request/Reply theHardwareType:1, theProtocolType:800, theHardwareSize:4, theProtocolSize:0, theOpcode=2, senderMac:00:11:22:33:44:AB, senderIp:192.168.100.100, vni:100

debug interface adsl events

Use the **debug interface adsl events** command to activate debug messages associated with asymmetric digital subscriber line (ADSL) events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example activates debug messages for ADSL events:

```
>enable
#debug interface adsl events
```

debug interface cellular

Use the **debug interface cellular** command to activate debug messages associated with the cellular interface. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug interface cellular
debug interface cellular <*slot/port*>
debug interface cellular <*slot/port*> **data**
debug interface cellular <*slot/port*> **data-hdlc**
debug interface cellular <*slot/port*> **diag-hdlc**
debug interface cellular <*slot/port*> **diagnostic**
debug interface cellular <*slot/port*> **diagnostic rx**
debug interface cellular <*slot/port*> **diagnostic tx**
debug interface cellular <*slot/port*> **diagnostic both**
debug interface cellular <*slot/port*> **download**

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*slot/port*>	Optional. Activates debug messages for the specified cellular interface.
data	Optional. Activates debug messages for the handshaking signals on the data channel.
data-hdlc	Optional. Activates debug messages for high level data link control (HDLC) errors on the data channel.
diag-hdlc	Optional. Activates debug messages for HDLC errors on the diagnostic channel.
diagnostic	Optional. Activates debug messages for all packets.
diagnostic rx	Optional. Activates debug messages for packets moving from the cellular interface to the network.
diagnostic tx	Optional. Activates debug messages for packets moving from the network to the cellular interface.
diagnostic both	Optional. Activates debug messages for both transmitted and received packets.
download	Optional. Activates debug messages for application downloads.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.2	Command was introduced.
Release 17.4	Command was expanded to include the keyword **both**.

Usage Examples

The following example activates error and event debug messages associated with the cellular interface:

>**enable**
#debug interface cellular

debug interface cellular modem messaging

Use the **debug interface cellular modem messaging** command to activate debug messages associated with messages going to or from the cellular modem. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug interface cellular modem messaging
debug interface cellular modem messaging detail
debug interface cellular modem messaging include-polled
debug interface cellular modem messaging include-polled detail

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

detail	Optional. Specifies that detailed information about messages going to or from the modem is included in the debug message.
include-polled	Optional. Specifies that polled messages going to and from the modem are included in the debug message.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.9.0	Command was introduced.

Usage Examples

The following example activates debug messages associated with messages going to or from the cellular modem:

>enable
#debug interface cellular modem messaging

debug ip access-list *<name>*

Use the **debug ip access-list** command to activate debug messages for a specific Internet Protocol version 4 (IPv4) access control list (ACL). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

<name>	Specifies a configured IPv4 ACL.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 6.1	Command was introduced.
Release R10.2.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

The **debug ip access-list** command provides debug messages to aid in troubleshooting IPv4 ACL issues. These debug messages are populated by traffic matches that occur when traffic is filtered through the ACL. The ACL must have the logging feature enabled in order to populate the debug message. To enable ACL match logging, refer to the *IPv4 Access Control List Command Set on page 4252*.

Usage Examples

The following is sample output of debug messages for the IPv4 ACL labeled **MatchAll**:

```
>enable
#debug ip access-list MatchAll
2009.06.09 14:15:03 ACCESS_LIST.MatchAll      permit host 192.168.0.1 log (1 matches)
2009.06.09 14:15:13 ACCESS_LIST.MatchAll      permit host 192.168.0.1 log (3 matches)
2009.06.09 14:15:57 ACCESS_LIST.MatchAll      permit host 192.168.0.1 log (1 matches)
```


debug ip crypto ipsec

Use the **debug ip crypto ipsec** command to activate debug messages associated with Internet Protocol security (IPsec) functions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.5.0	Command was introduced. This command replaces the **debug crypto ipsec** command.

Usage Examples

The following example activates the IPsec debug messages:

```
>enable
#debug ip crypto ipsec
```


debug ip dhcp client

Use the **debug ip dhcp client** command to activate debug messages associated with Dynamic Host Configuration Protocol version 4 (DHCPv4) client operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip dhcp client
debug ip dhcp client <*interface*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*interface*>	Optional. Specifies an interface to which an IPv4 address can be assigned in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **debug ip dhcp-client ?** for a list of valid interfaces.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 2.1	Command was introduced.
Release 16.1	Command was expanded to include the **interface** parameter.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release 18.3	Command syntax was changed to remove the hyphen (from **dhcp-client**) for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen (from **dhcp-client**) for Adtran voice products.

Functional Notes

The **debug ip dhcp client** command activates debug messages to provide information on DHCPv4 client activity in AOS. The AOS DHCPv4 client capability allows interfaces to dynamically obtain an IPv4 address from a network DHCPv4 server.

Usage Examples

The following example activates debug messages associated with DHCPv4 client activity:

>**enable**
#debug ip dhcp client

debug ip dhcp relay

Use the **debug ip dhcp relay** command to activate debug messages associated with Dynamic Host Configuration Protocol version 4 (DHCPv4) relay operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip dhcp relay
debug ip dhcp relay vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

vrf <*name*>	Optional. Displays debug information for the specified virtual routing and forwarding (VRF) instance.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 18.2	Command was introduced.
Release 18.3	Command syntax was changed to remove the hyphen (from **dhcp-relay**) for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen (from **dhcp-relay**) for Adtran voice products.

Functional Notes

The **debug ip dhcp relay** command activates debug messages to provide information on DHCPv4 relay activity in AOS. The AOS DHCPv4 relay capability allows AOS to relay DHCPv4 messages to a configured destination on the network.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates debug messages associated with DHCPv4 server activity only on the default VRF instance:

>enable
#debug ip dhcp relay

debug ip dhcp server

Use the **debug ip dhcp server** command to activate debug messages associated with Dynamic Host Configuration Protocol version 4 (DHCPv4) server operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip dhcp server
debug ip dhcp server vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

vrf <*name*>	Optional. Displays debug information for the specified virtual routing and forwarding (VRF) instance.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 2.1	Command was introduced.
Release 17.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command syntax was changed to remove the hyphen (from **dhcp-server**) for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen (from **dhcp-server**) for Adtran voice products.

Functional Notes

The **debug ip dhcp server** command activates debug messages to provide information on DHCPv4 server activity in AOS. The AOS DHCPv4 server capability allows AOS to dynamically assign IPv4 addresses to hosts on the network.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates debug messages associated with DHCPv4 server activity only on the default VRF instance:

>**enable**
#debug ip dhcp server

debug ip ffe wildcards

Use the **debug ip ffe wildcards** command to enable debug messaging for Internet Protocol version 4 (IPv4) RapidRoute wildcard events. This command can be used to determine which of several subsystem configurations caused a specific RapidRoute wildcard to be disabled.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.You can view wildcard status on a per-interface basis using the command* *show ip ffe on page 708*.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

When RapidRoute wildcard debug messages are enabled, two wildcard events are displayed. A **calculate** event, generated when an interface is called to recalculate its inbound or outbound wildcards, displays the results for each subsystem in the order in which wildcard processing is completed. A **finalize set** event is generated when the complete wildcards for an interface are pushed to either hardware or software processing and the new wildcards are used.

The order of wildcard bits displayed in a wildcard debug message are the opposite of the order displayed in the **show ip ffe wildcard** command, and exclude the Destination IP Address (which cannot be wildcarded). The last bit displayed at the end of the wildcard string is the least significant bit and represents the Source IP Address.

Usage Examples

The following example enables RapidRoute wildcard debug messaging and provides sample event output. Also included in the example are the configuration of the IPv4 access control list (ACL) named **ACL** and its application to the gigabit Ethernet subinterface **0/5.1**:

```
>enable
#debug ip ffe wildcards
#config t
(config)#ip access-list extended ACL
(config-ext-nacl)#permit icmp any any echo
(config-ext-nacl)#exit
(config)#interface gigabit ethernet 0/5.1
(config-giga-eth 0/5.1)#ip access-group ACL out
```



```
2015.01.01 12:00:34 FFEWILDCARDV4.giga-eth 0/5.1 calculate outbound:
    QoS:                    11111111111
    AccessGroup:            11011110111
2015.01.01 12:00:34 FFEWILDCARDV4.Loopback finalize set: 11011110111
2015.01.01 12:00:34 FFEWILDCARDV4.null 0 finalize set: 11011110111
2015.01.01 12:00:34 FFEWILDCARDV4.giga-eth 0/2.1 finalize set: 11011110111
2015.01.01 12:00:34 FFEWILDCARDV4.giga-eth 0/5.1 finalize set: 11011110111
```

debug ip firewall

Use the **debug ip firewall** command to activate debug messages associated with the AOS Internet Protocol version 4 (IPv4) firewall operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip firewall
debug ip firewall vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

vrf <*name*>	Optional. Displays debug information for the specified virtual routing and forwarding (VRF) instance.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 2.1	Command was introduced.
Release 17.1	Command was expanded to include the **vrf** parameter.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

The **debug ip firewall** command activates debug messages to provide real-time information about the IPv4 AOS stateful inspection firewall operation.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates the debug messages for the IPv4 AOS stateful inspection firewall:

>enable
#debug ip firewall

The following example activates the IPv4 firewall debug messages for the VRF instance **gray** and provides sample output:

>**enable**
#debug ip firewall vrf gray

2000.05.11 19:29:04 FIREWALL_VRF.Gray SrcPort: 41801, DstPort: 80
2000.05.11 19:29:04 FIREWALL_VRF.Gray Selector2: Dir=Public, int=vlan 309, Protocol=6, VRF Black cookie-> vlan 306
2000.05.11 19:29:04 FIREWALL_VRF.Gray SrcIp: 192.168.10.140, DstIp: 192.168.9.6
2000.05.11 19:29:04 FIREWALL_VRF.Gray SrcPort: 80, DstPort: 41801
2000.05.11 19:29:04 FIREWALL_VRF.Gray Deleting Association
2000.05.11 19:29:04 FIREWALL_VRF.Gray Assoc Index = 6242787, Count (total, policy-class) = 127, 126
2000.05.11 19:29:04 FIREWALL_VRF.Gray nat source -> 192.168.9.6, flags = 0x2000003F, 0x00000004, timeout = 6

debug ip firewall alg sip

Use the **debug ip firewall alg sip** command to activate debug messages associated with Session Initiation Protocol (SIP) information with AOS firewall operation. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip firewall alg sip
debug ip firewall alg sip packets
debug ip firewall alg sip verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

packets	Optional. Activates firewall application-level gateway (ALG) SIP packet debug messages.
verbose	Optional. Activates detailed debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.3	Command was introduced.
Release A1	Command was expanded to include the **packets** parameter.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Usage Examples

The following example activates debug messages associated with SIP information with AOS firewall operation:

>**enable**
#debug ip firewall alg sip

debug ip flow

Use the **debug ip flow** command to display debug messages associated with integrated traffic monitoring (ITM) operation. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip flow cache entry
debug ip flow cache expiration
debug ip flow export

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

cache entry	Specifies a debug message will be generated every time traffic flow data is added to the flow cache.
cache expiration	Specifies a debug message will be generated every time traffic flow data expires from the flow cache.
export	Specifies a debug message will be generated every time a message is sent to an external data collector.

Default Values

By default, debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables debug messages for the **ip flow export** command and gives sample output:

```
#debug ip flow export
#show run
    ip flow export destination 10.22.22.254 3000
    ip flow export vrf BLUE destination 172.16.4.5 65774

*Dec 18 22:45:43: IPFLOW: Sent export pkt #32958 to 10.22.22.254:3000
*Dec 18 22:45:43: IPFLOW: Sent export pkt #32958 to 172.16.4.5:65774 (BLUE)
```

The following is sample output from the **debug ip flow cache expiration** command:

```
#debug ip flow cache expiration
#show run
interface shdsl 2/1
    16:38:37: FLOW.CACHE: Expired 10.23.197.244:23 > 172.22.77.208: 1188 out eth 0/1 <T=0/P=6>
    16:38:37: FLOW.CACHE: ^Idle Time = 60, Active Time = 60
interface adsl 1/1
    16:39:20: FLOW.CACHE: Expired 10.23.197.244.23 > 172.22.77.208:1189 out eth 0/1 <T=0/P=6>
    16:39:20: FLOW.CACHE: ^Idle Time = 60, Active Time = 90
```

The following is sample output from the **debug ip flow cache entry** command:

```
#debug ip flow cache entry
#show run
    16:52:20: FLOW.CACHE: Added 172.22.77.208: 1189 > 10.23.197.244: 23 in eth 0/1 <T=0/P=6>
```


debug ip ftp-server

Use the **debug ip ftp-server** command to activate debug messages associated with File Transfer Protocol (FTP) server events in the AOS device. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 13.1	Command was introduced.

Functional Notes

The **debug ip ftp-server** command activates debug messages to provide information on FTP server activity in AOS. The FTP server capability allows for fast file management and transport for local or remote devices.

Usage Examples

The following example activates debug messages associated with FTP server activity:

```
>enable
#debug ip ftp-server
```

debug ip icmp

Use the **debug ip icmp** command to show all Internet Control Message Protocol (ICMP) version 4 (ICMPv4) messages as they come into the router or are originated by the router. If an optional keyword (**send** or **recv**) is not used, all results are displayed. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip icmp
debug ip icmp send
debug ip icmp recv

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

send	Optional. Displays only ICMPv4 messages sent by the router.
recv	Optional. Displays only ICMPv4 messages received by the router.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example activates the **debug ip icmp** send and receive messages for ICMPv4 in AOS:

>enable
#debug ip icmp
ICMP SEND: From (0.0.0.0) to (172.22.14.229) Type=8 Code=0 Length=72 Details:echo request
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=0 Code=0 Length=72 Details:echo reply
ICMP SEND: From (0.0.0.0) to (172.22.14.229) Type=8 Code=0 Length=72 Details:echo request
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=0 Code=0 Length=72 Details:echo reply
ICMP RECV: From (172.22.255.200) to (10.100.23.19) Type=11 Code=0 Length=36 Details:TTL equals 0 during transit
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=3 Code=3 Length=36 Details:port unreachable
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=3 Code=3 Length=36 Details:port unreachable

debug ip igmp

Use the **debug ip igmp** command to enable debug messages for Internet Group Management Protocol (IGMP) transactions (including helper activity). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip igmp
debug ip igmp <*ip address*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*ip address*>	Optional. Specifies the IP address of a multicast group. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables IGMP debug messages for the specified multicast group:

>**enable**
#debug ip igmp 224.1.1.1

debug ip igmp snooping

Use the **debug ip igmp snooping** command to enable debug messages for Internet Group Management Protocol (IGMP) snooping errors and events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip igmp snooping
debug ip igmp snooping verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

verbose	Optional. Enables detailed debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example enables IGMP snooping debug messages:

>enable
#debug ip igmp snooping

debug ip mrouting

Use the **debug ip mrouting** command to activate debug messages associated with multicast table routing events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following sample activates **ip mrouting** debug messages:

```
>enable
#debug ip mrouting
```

debug ip nhrp

Use the **debug ip nhrp** command to activate debug messages associated with Next Hop Resolution Protocol (NHRP) operations. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip nhrp
debug ip nhrp events
debug ip nhrp packets

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

events	Optional. Limits output to NHRP events.
packets	Optional. Limits output to NHRP packets.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.7.0	Command was introduced.

Usage Examples

The following example enables debug messages associated with NHRP:

```
>enable
#debug ip nhrp
18:21:32 NHRP tunnel 1: No reply for registration request to 10.10.10.254 after 16s, resending
18:21:33 NHRP tunnel 1: Error indication received from 10.10.10.254
```


debug ip ospf

Use the **debug ip ospf** command to activate debug messages associated with Open Shortest Path First version 2 (OSPFv2) routing operations. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip ospf
debug ip ospf adj
debug ip ospf database-timer
debug ip ospf events
debug ip ospf flood
debug ip ospf hello
debug ip ospf lsa-generation
debug ip ospf packet
debug ip ospf retransmission
debug ip ospf spf
debug ip ospf tree

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

adj	Optional. Displays OSPF adjacency events.
database-timer	Optional. Displays OSPF database timer.
events	Optional. Displays OSPF events.
flood	Optional. Displays OSPF flooding.
hello	Optional. Displays OSPF hello events.
lsa-generation	Optional. Displays OSPF link state advertisement (LSA) generation.
packet	Optional. Displays OSPF packets.
retransmission	Optional. Displays OSPF retransmission events.
spf	Optional. Displays OSPF shortest path first (SPF) calculations.
tree	Optional. Displays OSPF database tree.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following is an example of **debug ip ospf** command results:

>**enable**
#debug ip ospf flood
OSPF: Update LSA: id=c0a8020d rtid=192.168.2.13 area=11.0.0.0 type=1
OSPF: Update LSA: id=0b003202 rtid=11.0.50.2 area=11.0.0.0 type=1
OSPF: Queue delayed ACK lasid=0b003202 lsartid=11.0.50.2 nbr=11.0.50.2
OSPF: Rx ACK lasid=c0a8020d lsartid=192.168.2.13 nbr=11.0.50.2
OSPF: Received LSA ACK LSA_ID=-64.-88.2.13 LSA_RT_ID=-64.-88.2.13
OSPF: Rx ACK lasid=00000000 lsartid=192.168.2.13 nbr=11.0.50.2
OSPF: Received LSA ACK LSA_ID=0.0.0.0 LSA_RT_ID=-64.-88.2.13
OSPF: Sending delayed ACK
OSPF: Update LSA: id=c0a8020d rtid=192.168.2.13 area=11.0.0.0 type=1
OSPF: Flooding out last interface
OSPF: Update LSA: id=0b003202 rtid=11.0.50.2 area=11.0.0.0 type=1

debug ip packet

Use the **debug ip packet** command to display debug messages for every Internet Protocol version 4 (IPv4) packet forwarded through the unit. Adding the VRF name to this command displays debug information only for the named virtual routing and forwarding (VRF) instance. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip packet
debug ip packet detail
debug ip packet dump
debug ip packet <*ipv4 acl name*>
debug ip packet <*ipv4 acl name*> **detail**
debug ip packet <*ipv4 acl name*> **dump**
debug ip packet any-vrf
debug ip packet any-vrf <*ipv4 acl name*>
debug ip packet any-vrf <*ipv4 acl name*> **detail**
debug ip packet any-vrf <*ipv4 acl name*> **dump**
debug ip packet any-vrf detail
debug ip packet any-vrf dump
debug ip packet vrf <*name*>
debug ip packet vrf <*name*> <*acl name*>
debug ip packet vrf <*name*> <*acl name*> **detail**
debug ip packet vrf <*name*> <*acl name*> **dump**
debug ip packet vrf <*name*> **detail**
debug ip packet vrf <*name*> **dump**

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

detail	Optional. Displays IPv4 packet detailed information.
dump	Optional. Displays IPv4 packet detailed information, as well as a hex dump of the packets payload. **Note**: The console stream can be captured to a log file and used as an input file for display with ETHEREAL/Wireshark by using **text2pcap.exe**, which is a part of the ETHEREAL/Wireshark distribution. Execute as follows: **text2pcap -l 101** <*input_file*> <*output_file*>

	Next, open the output file with ETHEREAL/Wireshark for display and decode. The typical lower layer information in ETHEREAL/Wireshark may not be present. This converted capture file is treated as a raw IP capture and also has no timestamp data. Remember to take advantage of access control lists (ACLs) to narrow down the amount of data being processed with this facility. This is a CPU-intensive operation, and also disables any fast flow/fast cache routing.
<ipv4 acl name>	Optional. Displays debug information for a specific IPv4 ACL.
any-vrf	Optional. Displays debug information for all VRFs, including the default.
vrf *<name>*	Optional. Displays debug information for the specified VRF.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 12.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output for the **debug ip packet** command, which provides debug information for the default VRF only:

>**enable**
#debug ip packet

IP: s= 192.168.8.101 (eth 0/1) d=192.168.7.2 (eth 0/2) g= 192.168.7.2, forward
IP: s= 192.168.7.2 (eth 0/2) d=192.168.8.101 (eth 0/1) g= 192.168.8.101, forward
IP: s= 192.168.8.101 (eth 0/1) d=192.168.7.2 (eth 0/2) g= 192.168.7.2, forward
IP: s= 192.168.7.2 (eth 0/2) d=192.168.8.101 (eth 0/1) g= 192.168.8.101, forward

Where:

s=192.168.8.101 (eth 0/1) indicates source address and interface of received packet.
d=192.168.7.2 (eth 0/2) indicates destination address and interface from which the packet is being sent.
g=192.168.7.2 indicates the address of the next-hop gateway.
forward indicates the router is forwarding this packet.

The following is sample output for the **debug ip packet vrf** <*name*> command for the VRF named **Red**:

```
>enable
#debug ip packet vrf RED

IP: s=192.168.1.100 (eth 0/1.4) d=192.168.1.255 (Loopback), vrf=RED, rcvd
IP: s=192.168.1.101 (eth 0/1.4) d=192.168.1.1 (Loopback), vrf=RED, rcvd
IP: s=192.168.1.1 (Loopback) d=192.168.1.101 (eth 0/1.4) g=192.168.1.101, vrf=RED, forward
IP: s=192.168.1.100 (eth 0/1.4) d=192.168.1.1 (Loopback), vrf=RED, rcvd
IP: s=192.168.1.1 (Loopback) d=192.168.1.100 (eth 0/1.4) g=192.168.1.100, vrf=RED, forward
```

Where:

rcvd indicates the router received this packet.

The following is sample output for the **debug ip packet any-vrf** command:

```
>enable
#debug ip packet any-vrf

IP: s=192.168.1.15 (eth 0/1.1) d=192.168.1.1 (Loopback), rcvd
IP: s=192.168.1.1 (Loopback) d=192.168.1.15 (eth 0/1.1) g=192.168.1.15, forward
IP: s=192.168.1.101 (eth 0/1.4) d=255.255.255.255 (Loopback), vrf=RED, rcvd
IP: s=192.168.1.1 (Loopback) d=192.168.1.101 (eth 0/1.4) g=192.168.1.101, vrf=RED, forward
IP: s=192.168.2.33 (eth 0/1.3) d=192.168.2.1 (Loopback), vrf=BLU, rcvd
IP: s=192.168.2.1 (Loopback) d=192.168.2.33 (eth 0/1.3) g=192.168.2.33, vrf=BLU, forward
IP: s=192.168.1.101 (eth 0/1.4) d=192.168.1.1 (Loopback), vrf=RED, rcvd
IP: s=192.168.1.1 (Loopback) d=192.168.1.101 (eth 0/1.4) g=192.168.1.101, vrf=RED, forward
```

Where:

if the **vrf=**<*name*> statement is not present, the packet was present on the default VRF.
vrf=<*name*> indicates the nondefault VRF from which the packet was received.
forward indicates the router transmitted this packet.
g=x.x.x.x indicates the next-hop IP address to which the packet was forwarded.

debug ip pim-sparse

Use the **debug ip pim-sparse** command to display all protocol-independent multicast (PIM) sparse mode information. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all PIM sparse mode messages:

```
>enable
#debug ip pim-sparse
```


debug ip pim-sparse assert

Use the **debug ip pim-sparse assert** command to display debug messages associated with protocol-independent multicast (PIM) sparse assert transactions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip pim-sparse assert
debug ip pim-sparse assert event
debug ip pim-sparse assert event <*multicast address*>
debug ip pim-sparse assert state
debug ip pim-sparse assert state <*multicast address*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

event	Optional. Displays PIM sparse assert events.
state	Optional. Displays PIM sparse assert state changes.
<*multicast address*>	Optional. Specifies multicast group IP address to filter. The multicast group IP address range is **244.0.0.0** to **239.255.255.255** or **224.0.0.0 /4**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all PIM sparse assert event messages:

>enable
#debug ip pim-sparse assert event
14:25:05: PIMSM: Assert - MRoute (*, 239.255.255.250, eth 0/2) processed Received Join in NoInfo state
14:25:29: PIMSM: Assert - MRoute (10.100.13.240, 239.192.19.136, eth 0/2) processed Received Join in NoInfo state
14:25:29: PIMSM: Assert - MRoute (*, 239.192.19.136, eth 0/2) processed Received Join in NoInfo state
14:26:05: PIMSM: Assert - MRoute (*, 239.255.255.250, eth 0/2) processed Received Join in NoInfo state

debug ip pim-sparse hello

Use the **debug ip pim-sparse hello** command to display protocol-independent multicast (PIM) sparse mode hello transactions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates PIM sparse mode hello messages:

```
>enable
#debug ip pim-sparse hello
```

debug ip pim-sparse joinprune

Use the **debug ip pim-sparse joinprune** command to display protocol-independent multicast (PIM) sparse mode join and prune transactions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip pim-sparse joinprune
debug ip pim-sparse joinprune event
debug ip pim-sparse joinprune event <*multicast address*>
debug ip pim-sparse joinprune state
debug ip pim-sparse joinprune state <*multicast address*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

event	Optional. Displays PIM sparse join and prune events.
state	Optional. Displays PIM sparse join and prune state changes.
<*multicast address*>	Optional. Specifies multicast group IP address to filter. The multicast group IP address range is **244.0.0.0** to **239.255.255.255** or **224.0.0.0 /4**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates PIM sparse mode messages for all join and prune events and state changes:

>enable
#debug ip pim-sparse joinprune
14:27:05: PIMSM: Processed JOIN(*, 239.255.255.250) from 10.10.10.2
14:27:29: PIMSM: Processed JOIN(10.100.13.240, 239.192.19.136) from 10.10.10.2
14:27:29: PIMSM: Processed JOIN(*, 239.192.19.136) from 10.10.10.2
14:27:56: PIMSM: Sent JOIN(10.100.13.240, 239.192.19.136) to 10.100.13.240
14:28:05: PIMSM: Processed JOIN(*, 239.255.255.250) from 10.10.10.2

debug ip pim-sparse packets

Use the **debug ip pim-sparse packets** command to display protocol-independent multicast (PIM) sparse mode packet information. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.Variations of this command include:

debug ip pim-sparse packets
debug ip pim-sparse packets in
debug ip pim-sparse packets in *<interface>*
debug ip pim-sparse packets out
debug ip pim-sparse packets out *<interface>*

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

in	Optional. Displays messages for inbound PIM sparse packets.
out	Optional. Displays messages for outbound PIM sparse packets.
<interface>	Optional. Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **debug ip pim-sparse packets ?** for a list of valid interfaces.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Usage Examples

The following example activates all PIM sparse packet messages (both inbound and outbound):

>enable
#debug ip pim-sparse packets

debug ip pim-sparse register

Use the **debug ip pim-sparse register** command to display protocol-independent multicast (PIM) sparse source registration messages. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip pim-sparse register
debug ip pim-sparse register event
debug ip pim-sparse register event <*multicast address*>
debug ip pim-sparse register state
debug ip pim-sparse register state <*multicast address*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

event	Optional. Displays PIM sparse register events.
state	Optional. Displays PIM sparse register state changes.
<*multicast address*>	Optional. Specifies multicast group IP address to filter. The multicast group IP address range is **244.0.0.0** to **239.255.255.255** or **224.0.0.0 /4**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all PIM sparse registration changes:

>enable
#debug ip pim-sparse register
18:14:22: PIMSM: Registered new source (10.100.13.240, 239.192.19.136) from 10.10.10.1
18:14:22: PIMSM: RegisterStop(10.100.13.240, 239.192.19.136) sent to 10.10.10.1
18:14:53: PIMSM: RegisterStop(10.100.13.240, 239.192.19.136) sent to 10.10.10.1
18:16:17: PIMSM: RegisterStop(10.100.13.240, 239.192.19.136) sent to 10.10.10.1

debug ip policy

Use the **debug ip policy** command to display policy-based routing events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug ip policy
debug ip policy <*acl name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*acl name*>	Optional. Displays debug information only for the specified access control list (ACL).

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.
Release 16.1	Command was expanded to filter based on an ACL.

Usage Examples

The following example creates a standard ACL named **PVT**, which permits packets sourced from the 10.22.0.0/16 network and displays only these policy-based routing event messages:

>enable
#ip access-list standard PVT
#permit 10.22.0.0 0.0.255.255
#deny any
#debug ip policy PVT

debug ip rip

Use the **debug ip rip** command to activate debug messages associated with Routing Information Protocol (RIP) operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip rip
debug ip rip events

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

events	Optional. Displays only RIP protocol events.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **debug ip rip** command activates debug messages to provide information on RIP activity in AOS. RIP allows hosts and routers on a network to exchange information about routes.

Usage Examples

The following example activates debug messages associated with RIP activity:

>enable
#debug ip rip

debug ip route-cache express

Use the **debug ip route-cache express** command to activate debug messages associated with Layer 3 switching.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following is sample output for this command:

```
>enable
#debug ip route-cache express
xRt: Periodic ARP for 10.2.42.254
xRt: Processed 1 ARP events, with 0 remaining

xRt: host entry added: IP=192.168.1.10, MAC=00:10:94:00:00:01, Vlan=1
xRt: host entry added: IP=192.168.3.10, MAC=00:10:95:00:00:01, Vlan=3
xRt: host entry not added (no ARL entry): IP=192.168.5.10, MAC=00:10:96:00:00:01, Vlan=5
xRt: host entry added: IP=192.168.7.10, MAC=00:10:97:00:00:01, Vlan=7
xRt: host entry added: IP=192.168.9.10, MAC=00:10:98:00:00:01, Vlan=9
xRt: host entry added: IP=192.168.11.10, MAC=00:10:99:00:00:01, Vlan=11
xRt: host entry added: IP=192.168.13.10, MAC=00:10:9a:00:00:01, Vlan=13
xRt: host entry not added (no ARL entry): IP=192.168.15.10, MAC=00:10:9b:00:00:01, Vlan=15
xRt: host entry added: IP=192.168.17.10, MAC=00:10:9c:00:00:01, Vlan=17
xRt: host entry added: IP=192.168.19.10, MAC=00:10:9d:00:00:01, Vlan=19
xRt: Processed 10 ARP events, with 605 remaining
xRt: Processed 10 L2 events, with 393 remaining

xRt: host entry added (ARL entry found): IP=192.168.1.20, MAC=00:10:94:00:00:0b, Vlan=1
xRt: host entry added (ARL entry found): IP=192.168.15.10, MAC=00:10:9b:00:00:01, Vlan=15
xRt: host entry added (ARL entry found): IP=192.168.3.18, MAC=00:10:95:00:00:09, Vlan=3
xRt: host entry added (ARL entry found): IP=192.168.3.41, MAC=00:10:95:00:00:20, Vlan=3
xRt: Processed 10 L2 events, with 217 remaining
--MORE--
```


debug ip routing

Use the **debug ip routing** command to activate debug messages associated with Internet Protocol version 4 (IPv4) routing table events. Adding the VRF name to this command displays debug information for the named virtual routing and forwarding (VRF). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug ip routing
debug ip routing vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

vrf <*name*>	Optional. Displays debug information only for the specified VRF. If a VRF is not specified, the default VRF is assumed.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 10.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates debug messages associated with IPv4 routing table events:

>enable
#debug ip routing

The following example activates the debug messages associated with IPv4 routing table events on the nondefault VRF named **RED** and provides sample output:

>**enable**
#debug ip routing vrf RED

ip route vrf RED 1.2.3.0 255.255.255.0 192.168.10.10
15:32:29: ROUTING: Add route for 1.2.3.0/24 nh=192.168.10.10 vrf=RED
15:32:29: ROUTING: Remove route for 1.2.3.0/24 nh=192.168.10.10 vrf=RED
15:32:29: ROUTING: Add route for 1.2.3.0/24 nh=192.168.10.10 vrf=RED
15:32:29: ROUTING: Remove route for 1.2.3.0/24 nh=192.168.10.10 vrf=RED
15:32:29: ROUTING: Add route for 1.2.3.0/24 nh=192.168.10.10 vrf=RED

Where:

nh=192.168.10.10 indicates the next-hop address.
vrf=RED indicates the nondefault VRF where the route is present.

debug ip security monitor

Use the **debug ip security monitor** command to activate debug messages associated with the IP security monitor. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.5	Command was introduced.

Functional Notes

The **debug ip security monitor** events include statistic collection associated with the timeline.

Usage Examples

The following is sample output for this command:

>**enable**
#debug ip security monitor
SECURITY_MONITOR.EVENTS Regular update: timeline interval scheduled to end at 23:00:16
SECURITY_MONITOR.EVENTS [curr=269095, sched=272343]
SECURITY_MONITOR.EVENTS Regular update: timeline interval scheduled to end at 23:00:16
SECURITY_MONITOR.EVENTS [curr=269154, sched=272343] **no debug ip security monitor**
#

debug ip tcp

Use the **debug ip tcp** command to activate debug messages associated with Transmission Control Protocol (TCP) state changes, session allocation and deallocation, and packet information (for example, sequence numbers, acknowledgement numbers, and packet length) in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip tcp
debug ip tcp events
debug ip tcp md5

These debug events are logged for packets that are sent or received from the router. Forwarded TCP packets are not included.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

events	Optional. Displays only messages regarding TCP state changes and TCP session allocation.
md5	Optional. Displays messages related to the TCP Message Digest 5 (MD5) authentication process.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 4.1	Command was introduced.
Release 9.1	Command was expanded to include the **md5** parameter.

Functional Notes

The debug events for this command are logged for packets that are sent or received from the router. Forwarded TCP packets are not included in the output.

In the **debug ip tcp events** output, TCB stands for TCP task control block. The numbers which sometimes appear next to TCB (e.g., **TCB5** in the following example) represent the TCP session number. This allows you to differentiate debug messages for multiple TCP sessions.

Output for the **debug ip tcp md5** command can include messages such as: *MD5 authentication was expected but not received, MD5 authentication was not expected but was received, MD5 authentication failed, and MD5 authentication passed.* Debug messages will only be generated for TCP ports that have MD5 authentication enabled.

Usage Examples

The following is sample output for this command:

>**enable**
#debug ip tcp events
2003.02.17 07:40:56 IP.TCP EVENTS TCP: Allocating block 5
2003.02.17 07:40:56 IP.TCP EVENTS TCB5: state change: FREE->SYNRCVD
2003.02.17 07:40:56 IP.TCP EVENTS TCB5: new connection from 172.22.75.246:3473 to 10.200.2.201:23
2003.02.17 07:40:56 IP.TCP EVENTS TCB5: state change: SYNRCVD->ESTABLISHED [172.22.75.246:3473]
2003.02.17 07:41:06 IP.TCP EVENTS TCB5: Connection aborted -- error = RESET
2003.02.17 07:41:06 IP.TCP EVENTS TCB5: De-allocating tcb

debug ip tftp

Use the **debug ip tftp** command to activate debug messages associated with Trivial File Transfer Protocol (TFTP) packets. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip tftp client packets
debug ip tftp server events
debug ip tftp server packets

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

client packets	Activates TFTP client packet debug messages.
server events	Activates TFTP server event debug messages.
server packets	Activates TFTP server packet debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.
Release 14.1	Command changed from **debug tftp** to **debug ip tftp**.

Usage Examples

The following example activates debug messages associated with TFTP server packets:

>enable
#debug ip tftp server packets

debug ip udp

Use the **debug ip udp** command to activate debug messages associated with User Datagram Protocol (UDP) send and receive events in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

These debug events are logged for packets that are sent or received from the router. Forwarded UDP packets are not included.

The overhead associated with this command takes up a large portion of your router's resources and at times can halt other router processes. It is best to only use the command during times when the network resources are in low demand (nonpeak hours, weekends, etc.).

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 4.1	Command was introduced.

Functional Notes

In the **debug ip udp** information, the message **no listener** means that there is no service listening on this UDP port (i.e., the data is discarded).

Usage Examples

The following is sample output for this command:

```
>enable
#debug ip udp
2003.02.17 07:38:48 IP.UDP RX: src=10.200.3.236:138, dst=10.200.255.255:138, 229 bytes, no listener
2003.02.17 07:38:48 IP.UDP RX: src=10.200.2.7:138, dst=10.200.255.255:138, 227 bytes, no listener
2003.02.17 07:38:48 IP.UDP RX: src=10.200.201.240:138, dst=10.200.255.255:138, 215 bytes, no
    listener
```


debug ip urlfilter

Use the **debug ip urlfilter** command to display a summary of debug information for all uniform resource locator (URL) filters being used. Debug messages are displayed (real time) to the terminal (or Telnet) screen. The verbose option gives more detailed information. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ip urlfilter
debug ip urlfilter verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

verbose	Optional. Enables detailed debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example shows the debug summary for all URL filters being used:

>enable
#debug ip urlfilter

2005.11.06 05:31:52 Connected to a Websense server
2005.11.06 05:33:26 Allowed http://www.adtran.com/

debug ip urlfilter top-websites

Use the **debug ip urlfilter top-websites** command to display the times at which the generated top websites lists merge (as the 15-minute list is rolled into the hourly list, the hourly list into the daily list, and so on). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example shows the debug summary for top websites reporting:

```
>enable
#debug ip urlfilter top-websites
P2007.05.08 09:55:00 Merging displayed 15 minute list into hour list
2007.05.08 09:55:00 Merging hour list into twenty-four hour list
2007.05.08 09:55:00 Validating timers; timerAdj=0, update=0, lastThen=462
2007.05.08 09:55:00 Scheduled next run in 900; timerAdj=0, nowUpTime=462,
last Period=306
```


debug ipv6 crypto ipsec

Use the **debug ipv6 crypto ipsec** command to activate debug messages associated with Internet Protocol version 6 (IPv6) IP security (IPsec) events within the cryptographic subsystem. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 crypto ipsec
debug ipv6 crypto ipsec vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

vrf <*name*>	Optional. Displays debug information for the specified virtual routing and forwarding (VRF) instance. If no VRF is specified, information for the default VRF is displayed.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates the debug messages for IPv6 cryptographic subsystem processing:

>**enable**
#debug ipv6 crypto ipsec

debug ipv6 dhcp

Use the **debug ipv6 dhcp** command to enable debug messages for Dynamic Host Control Protocol version 6 (DHCPv6) operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 dhcp
debug ipv6 dhcp client
debug ipv6 dhcp client <*interface*>
debug ipv6 dhcp client mef-ethernet <*slot/port*>
debug ipv6 dhcp client system-control-evc
debug ipv6 dhcp client system-management-evc
debug ipv6 dhcp detail
debug ipv6 dhcp relay
debug ipv6 dhcp relay vrf <*name*>
debug ipv6 dhcp server
debug ipv6 dhcp server vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

client	Optional. Specifies that DHCPv6 client information is displayed.
<*interface*>	Optional. Specifies that only client information for the single interface is displayed. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.
mef-ethernet <*slot/port*>	Optional. Specifies that only client information for the Metro Ethernet Forum (MEF) Ethernet interface is displayed.
system-control-evc	Optional. Specifies that only client information for the system control Ethernet virtual connection (EVC) is displayed.
system-management-evc	Optional. Specifies that only client information for the system management EVC is displayed.
detail	Optional. Specifies that DHCPv6 packet content is displayed.
relay	Optional. Specifies that DHCPv6 relay information is displayed.
server	Optional. Specifies that DHCPv6 server information is displayed.
vrf <*name*>	Optional. Specifies that DHCPv6 server or relay information for a nondefault (named) virtual routing and forwarding (VRF) instance is displayed. If a VRF is not specified, information for the default VRF is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 18.3	Command was introduced.
Release R10.9.0	Command was expanded to include the **client** parameter.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R11.1.0	Command was expanded to include the **vrf** <*name*> parameter.

Usage Examples

The following example displays sample output for DHCPv6 relay debug information:

>**enable**
#debug ipv6 dhcp relay
2011.01.01 21:40:24 DHCPv6.RELAY Relaying SOLICIT from FE80::B098:1B0E:27CA:A8AB on eth 0/2
2011.01.01 21:40:24 DHCPv6.RELAY to FE80::2A0:C8FF:FE65:702 eth 0/1
2011.01.01 21:40:24 DHCPv6.RELAY Sending RELAY-FORWARD to FE80::2A0:C8FF:FE65:702 eth 0/1
2011.01.01 21:40:24 DHCPv6.RELAY Received RELAY-REPLY from FE80::2A0:C8FF:FE65:702 eth 0/1
2011.01.01 21:40:24 DHCPv6.RELAY Relaying RELAY-REPLY from FE80::2A0:C8FF:FE65:702 eth 0/1
2011.01.01 21:40:24 DHCPv6.RELAY to FE80::B098:1B0E:27CA:A8AB on eth 0/2
2011.01.01 21:40:24 DHCPv6.RELAY Sending REPLY to FE80::B098:1B0E:27CA:A8AB eth 0/2 on eth 0/2

debug ipv6 ffe wildcards

Use the **debug ipv6 ffe wildcards** command to enable debug messaging for Internet Protocol version 6 (IPv6) RapidRoute wildcard events. This command can be used to determine which of several subsystem configurations caused a specific RapidRoute wildcard to be disabled.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.You can view wildcard status on a per-interface basis using the command* *show ipv6 ffe on page 804*.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

When RapidRoute wildcard debug messages are enabled, two wildcard events are displayed. A **calculate** event, generated when an interface is called to recalculate its inbound or outbound wildcards, displays the results for each subsystem in the order in which wildcard processing is completed. A **finalize set** event is generated when the complete wildcards for an interface are pushed to either hardware or software processing and the new wildcards are used.

The order of wildcard bits displayed in a wildcard debug message are the opposite of the order displayed in the **show ipv6 ffe wildcard** command, and exclude the Destination IP Address (which cannot be wildcarded). The last bit displayed at the end of the wildcard string is the least significant bit and represents the Source IP Address.

Usage Examples

The following example enables RapidRoute wildcard debug messaging and provides sample event output. Also included in the example are the configuration of the IPv6 access control list (ACL) named **ACL** and its application to the gigabit Ethernet subinterface **0/5.1**:

>**enable**
#debug ipv6 ffe wildcards
#config t
(config)**#ipv6 access-list extended ACL**
(config-ext-nacl)**#permit icmpv6 any any echo**
(config-ext-nacl)**#exit**
(config)**#interface gigabit ethernet 0/5.1**
(config-giga-eth 0/5.1)**#ipv6 access-group ACL out**


```
2015.01.01 12:00:34 FFEWILDCARDV6.giga-eth 0/5.1 calculate outbound:
    QoS:                    11111111111
    AccessGroup:            11011110111
2015.01.01 12:00:34 FFEWILDCARDV6.Loopback finalize set: 11011110111
2015.01.01 12:00:34 FFEWILDCARDV6.null 0 finalize set: 11011110111
2015.01.01 12:00:34 FFEWILDCARDV6.giga-eth 0/2.1 finalize set: 11011110111
2015.01.01 12:00:34 FFEWILDCARDV6.giga-eth 0/5.1 finalize set: 11011110111
```


debug ipv6 firewall

Use the **debug ipv6 firewall** command to activate debug messages associated with AOS Internet Protocol version 6 (IPv6) firewall operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 firewall
debug ipv6 firewall vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

vrf <*name*>	Optional. Displays debug information for the specified virtual routing and forwarding (VRF) instance. If no VRF is specified, information for the default VRF is displayed.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates the debug messages for IPv6 firewall processing:

>**enable**
#debug ipv6 firewall

The following example activates the IPv6 firewall debug messages for the VRF instance **gray** and provides sample output:

>**enable**
#debug ipv6 firewall vrf gray

2010.08.17 20:39:25 FIREWALL_V6.VRF gray id=firewall time=”2010-08-17 20:39:25” fw=NV3430 pri=6 proto=icmpv6 src=2001:DB8:1:1::2 dst=2001:DB8:1:1::1 msg=”ICMPv6 type=128 code=0; Bytes processed over policy-session (bytes=256) from PRIVATEV6 policy-class on the interface eth 0/1.1”
2010.08.17 20:39:25 FIREWALL_V6.VRF gray Deleted policy-session due to clear all policy-sessions command
Policy-session ID = 2; Count (total, policy-class) = 0, 0
Protocol = 58; Flags = 0x1; Timeout = 60
Initiating side: Policy-class = PRIVATEV6
From/To: eth 0/1.1 -> Loopback
Source: 2001.DB8:1:1::2
Destination: 2001:DB8:1:1::1
ICMPv6 Type/Code: 128/0; ID: 0
Responding side: Policy-class = self
From/To: Loopback -> eth 0/1.1
Source: 2001:DB8:1:1::2
Destination: 2001:DB8:1:1::2
ICMPv6 Type/Code: 129/0; ID: 0

debug ipv6 firewall ndar

Use the **debug ipv6 firewall ndar** command to activate debug messages associated with AOS Internet Protocol version 6 (IPv6) firewall Neighbor Discovery (ND) operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 firewall ndar
debug ipv6 firewall vrf <*name*> **ndar**

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

ndar	Specifies that ND address resolution events are displayed.
vrf <*name*>	Optional. Displays debug information for the specified virtual routing and forwarding (VRF) instance. If no VRF is specified, information for the default VRF is displayed.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 18.3	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates the debug messages for IPv6 firewall ND address resolution processing on the default VRF instance:

>**enable**
#debug ipv6 firewall ndar

debug ipv6 icmp

Use the **debug ipv6 icmp** command to show all Internet Control Message Protocol (ICMP) version 6 (ICMPv6) messages being sent or received by the local IPv6 stack. For IPv6, these messages do not include ICMP packets being exchanged between other devices because those packets appear only as IPv6 packets (rather than ICMPv6 packets) to the local router. If an optional keyword (**send** or **recv**) is not used, all results are displayed. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 icmp
debug ipv6 icmp send
debug ipv6 icmp recv

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

send	Optional. Displays only ICMPv6 messages sent by the IPv6 stack.
recv	Optional. Displays only ICMPv6 messages received by the IPv6 stack.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example activates the **debug ipv6 icmp** send and receive messages for ICMPv6 in AOS:

```
>enable
#debug ipv6 icmp
ICMPv6 SEND: To [2001:DB8:8967::10] Type=128 Code=0 Length=108 Details:echo request
    id=0036 seq=0001
ICMPv6 SEND: Source changed to [2001:DB8:8967:1::100] before transmit
ICMPv6 RECV: From [1001:DB8:8967::10] to [2001:DB8:8967:1::100] [eth 0/1]
Type=129 Code=0 Length=108 Details: echo reply
    id=0036 seq=0001
--MORE--
```


debug ipv6 mld

Use the **debug ipv6 mld** command to display information related to Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) queries and responses. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 mld events
debug ipv6 mld events interface <*interface*>
debug ipv6 mld packet
debug ipv6 mld packet interface <*interface*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

events	Specifies that events related to MLD activity, such as timer starts or changes in compatibility mode, are displayed.
packet	Specifies that decoded packet information, including MLD message contents and associated MLD groups, are displayed.
interface <*interface*>	Optional. Limits command output to a specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.

Default Values

No default values are necessary for this command.

Command History

Release R11.4.0	Command was introduced.

Usage Examples

The following example displays sample output for MLD debug information:

```
>enable
#debug ipv6 mld
    2014.04.20 17:58:05 MLD.PKT giga-eth 0/2.1 Receive MLD packet, len=28
    type=130 (query), code=0, cksum=0x231d
    maxDelayMs=5000, mcast=:: (general)
    sFlag=0, QRV=2, QQIC=30, numSources=0
    2014.04.20 17:58:05 MLD.PKT giga-eth 0/2.1 Transmit MLD packet, len=88
    type=143 (v2 report), code=0, cksum=0x8f49
```


debug ipv6 named-prefix

Use the **debug ipv6 named-prefix** command to enable debug messages for all events associated with Internet Protocol version 6 (IPv6) named prefixes.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example enables debug messages for all IPv6 named prefixes:

```
>enable
#debug ipv6 named-prefix
```

debug ipv6 nd

Use the **debug ipv6 nd** command to activate debug messages for Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) functions on the router. This command details the processing of ND messages and all resulting state changes and errors. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 nd ar
debug ipv6 nd dad
debug ipv6 nd neighbor-state
debug ipv6 nd packet neighbor
debug ipv6 nd packet router

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

ar	Optional. Activates debug messaging for address resolution (AR) changes.
dad	Optional. Activates debug messaging for duplicate address detection (DAD) events.
neighbor-state	Optional. Activates debug messaging for state changes in the neighbor cache.
packet neighbor	Optional. Activates debug messaging for ND packets.
packet router	Optional. Activates debug messaging for router advertisement (RA) packets.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example activates debug messaging for all ND DAD events:

>**enable**
#debug ipv6 nd dad

debug ipv6 packet

Use the **debug ipv6 packet** command to display debug messages for every Internet Protocol version 6 (IPv6) packet forwarded through the unit. Adding the virtual routing and forwarding (VRF) instance name to this command displays debug information only for the named VRF instance. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ipv6 packet
debug ipv6 packet detail
debug ipv6 packet dump
debug ipv6 packet <*ipv6 acl name*>
debug ipv6 packet <*ipv6 acl name*> **detail**
debug ipv6 packet <*ipv6 acl name*> **dump**
debug ipv6 packet any-vrf
debug ipv6 packet any-vrf <*ipv6 acl name*>
debug ipv6 packet any-vrf <*ipv6 acl name*> **detail**
debug ipv6 packet any-vrf <*ipv6 acl name*> **dump**
debug ipv6 packet any-vrf detail
debug ipv6 packet any-vrf dump
debug ipv6 packet vrf <*name*>
debug ipv6 packet vrf <*name*> <*acl name*>
debug ipv6 packet vrf <*name*> <*acl name*> **detail**
debug ipv6 packet vrf <*name*> <*acl name*> **dump**
debug ipv6 packet vrf <*name*> **detail**
debug ipv6 packet vrf <*name*> **dump**

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

detail	Optional. Displays IPv6 packet detailed information.
dump	Optional. Displays IPv6 packet detailed information, as well as a hex dump of the packets payload.
<*ipv6 acl name*>	Optional. Displays debug information for a specific IPv6 access control list (ACL).
any-vrf	Optional. Displays debug information for all VRFs, including the default.
vrf <*name*>	Optional. Displays debug information for the specified VRF.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output for the **debug ipv6 packet** command, which provides debug information for the default VRF only:

>**enable**
#debug ip packet

IPv6: s=FE80::2A0:C8FF:FE00:6120 (Loopback)
d=FF02::5 (eth 0/1)
g=FF02::5
forward, size = 76(36)

IPv6: s=FE80::2A0:C8FF:FE00:6120 (Loopback)
d=2620:106:A001:899:4DC8:275B:34AA:99F6 (eth 0/1)
g=2620:106:A001:899:4DC8:275B:34AA:99F6
forward, size = 72(32)

In this example, the following is true:

s=FE80::2A0:C8FF:FE00:6120 (Loopback) indicates the source address and interface of received packet.
d=FF02::5 (eth 0/1) indicates the destination address and interface from which the packet is being sent.
g=FF02::5 indicates the address of the next-hop gateway.
forward indicates the router is forwarding this packet.

debug ipv6 routing

Use the **debug ipv6 routing** command to activate debug messages associated with Internet Protocol version 6 (IPv6) routing table events. Adding the VRF name to this command displays debug information for the named virtual routing and forwarding (VRF). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug ipv6 routing
debug ipv6 routing vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

vrf <*name*>	Optional. Displays debug information only for the specified VRF. If a VRF is not specified, the default unnamed VRF is assumed.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example activates debug messages associated with IPv6 routing table events:

>**enable**
#debug ipv6 routing

debug isdn

Use the **debug isdn** command to activate debug messages associated with integrated services digital network (ISDN) events in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug isdn cc-ie
debug isdn cc-ie bri
debug isdn cc-ie bri <*number*>
debug isdn cc-ie pri
debug isdn cc-ie pri <*number*>
debug isdn cc-messages
debug isdn cc-messages bri
debug isdn cc-messages bri <*number*>
debug isdn cc-messages pri
debug isdn cc-messages pri <*number*>
debug isdn endpoint
debug isdn endpoint bri
debug isdn endpoint bri <*number*>
debug isdn endpoint pri
debug isdn endpoint pri <*number*>
debug isdn interface
debug isdn interface bri
debug isdn interface bri <*number*>
debug isdn interface pri
debug isdn interface pri <*number*>
debug isdn l2-formatted
debug isdn l2-formatted bri
debug isdn l2-formatted bri <*number*>
debug isdn l2-formatted pri
debug isdn l2-formatted pri <*number*>
debug isdn l2-messages
debug isdn l2-messages bri
debug isdn l2-messages bri <*number*>
debug isdn l2-messages pri
debug isdn l2-messages pri <*number*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

bri	Optional. Specifies the basic rate interface (BRI) interface.
cc-ie	Displays call control information elements.

cc-messages	Displays call control messages.
endpoint	Displays endpoint events.
interface	Displays ISDN interface events.
l2-formatted	Displays Layer 2 formatted messages.
l2-messages	Displays Layer 2 messages.
pri	Optional. Specifies the ISDN interface.
pri <*number*>	Optional. Specifies a specific ISDN interface. Range is **1** to **255**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was expanded to include the **bri** parameter.

Usage Examples

The following example activates all Layer 2 formatted messages:

>**enable**
#debug isdn l2-formatted

The following example activates Layer 2 formatted messages received on ISDN interface primary rate interface (PRI) 1:

>**enable**
#debug isdn l2-formatted pri 1

debug isdn group

Use the **debug isdn group** command to activate integrated services digital network (ISDN) group errors and messages. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug isdn group
debug isdn group <*number*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*number*>	Optional. Specifies the ISDN group. Valid range is **1** to **255**.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages for all ISDN groups:

>enable
#debug isdn group

debug isdn resource-manager

Use the **debug isdn resource-manager** command to activate integrated services digital network (ISDN) resource manager errors and messages. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with the ISDN resource manager:

```
>enable
#debug isdn resource-manager
```


debug isdn verbose

Use the **debug isdn verbose** command to activate all debug messages associated with integrated services digital network (ISDN) events in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all debug messages associated with ISDN activity:

```
>enable
#debug isdn verbose
```

debug licensing

Use the **debug licensing** command to display licensing event messages. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.8.0	Command was introduced.

Usage Examples

The following example activates licensing event messages:

```
>enable
#debug licensing
```

debug lldp

Use the **debug lldp** command to display debug output for all Link Layer Discovery Protocol (LLDP) receive and transmit packets. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug lldp
debug lldp rx
debug lldp rx verbose
debug lldp tx
debug lldp tx verbose
debug lldp verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

rx	Optional. Shows information about received packets.
tx	Optional. Shows information about transmitted packets.
verbose	Optional. Shows detailed debugging information.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.
Release R11.5.0	Command was expanded to include inventory information if transmitted by the endpoint.

Usage Examples

The following example activates both transmit and receive messages associated with LLDP operation:

>enable
#debug lldp

debug mail-client

Use the **debug mail-client** command to enable mail agent debug messages. Variations of this command include:

debug mail-client
debug mail-client *<agent name>*

> *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

<agent name>	Optional. Specifies debug messages are enabled only for the specified mail agent.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example enables debug messaging for all configured mail agents:

>enable
#debug mail-client

debug mef config

Use the **debug mef config** command to enable debug messaging for all Metro Ethernet Forum (MEF) components configured on the unit. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug mef config
debug mef config detail

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

detail	Optional. Specifies that detailed debug information is displayed.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release A4.05	Command was introduced.

Usage Examples

The following example enables debug messages for all MEF component configurations:

>enable
#debug mef config

debug mgcp stack

Use the **debug mgcp stack** command to display information about the Media Gateway Control Protocol (MGCP) stack and MGCP messages. Variations of this command include:

debug mgcp stack
debug mgcp stack messages
debug mgcp stack messages summary
debug mgcp stack verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

messages	Optional. Specifies that MGCP stack messages information is displayed.
messages summary	Optional. Specifies that MGCP message summary information is displayed.
verbose	Optional. Specifies that detailed MGCP stack information is displayed.

Default Values

No default values are necessary for this command.

Command History

Release A2	Command was introduced.

Usage Examples

The following is sample output from the **debug mgcp stack messages summary** command:

```
#debug mgcp stack messages summary
19:20:22 MGCP.STACK MSGSUM TX: -> 47.234.101.60:2727
19:20:22 MGCP.STACK MSGSUM TX: ntfy 88 aaln/1@65.162.109.238 MGCP 1.0
19:20:22 MGCP.STACK MSGSUM RX: <- 47.234.101.60:2727
19:20:22 MGCP.STACK MSGSUM RX: 200 88 OK

19:20:22 MGCP.STACK MSGSUM RX: <- 47.234.101.60:2727
19:20:22 MGCP.STACK MSGSUM RX: RQNT 30425 aaln/1@65.162.109.238 MGCP 1.0
```


debug mgcp verbose

Use the **debug mgcp verbose** command to display detailed information about Media Gateway Control Protocol (MGCP) transmissions and receptions.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A2	Command was introduced.

Usage Examples

The following is sample output from the **debug mgcp verbose** command:

```
#debug mgcp verbose
19:02:35 MGCP.STACK DEBUG adEndpointEvent(int=0:1, pkg=, evt=hd)
19:02:35 MGCP.STACK MSG TX: -> 47.234.101.60:2727
19:02:35 MGCP.STACK MSG TX: ntfy 58 aaln/1@65.162.109.238 MGCP 1.0
                            K: 57
                            X: 22410
                            O: l/hd

19:02:35 MGCP.STACK MSG RX: <- 47.234.101.60:2727
19:02:35 MGCP.STACK MSG RX: 200 58 OK

19:02:35 MGCP.STACK MSG RX: <- 47.234.101.60:2727
19:02:35 MGCP.STACK MSG RX: RQNT 30081 aaln/1@65.162.109.238 MGCP 1.0
                            X: 22414
                            S:
                            R: L/hu(N)
                            Q: loop
```

debug network-forensics ip dhcp

Use the **debug network-forensics ip dhcp** command to display Dynamic Host Configuration Protocol (DHCP) information collected from messages sent between clients connected to the network and the network server. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Debug messages can be activated for all clients or for specific clients connected to the network. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug network-forensics ip dhcp
debug network-forensics ip dhcp hostname <*hostname*>
debug network-forensics ip dhcp interface gigabit-switchport <*slot/port*>
debug network-forensics ip dhcp interface switchport <*slot/port*>
debug network-forensics ip dhcp interface xgigabit-switchport <*slot/port*>
debug network-forensics ip dhcp ip <*ip address*>
debug network-forensics ip dhcp mac <*mac address*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

hostname <*hostname*>	Optional. Activates debug messages for the client with the specified host name.
interface gigabit-switchport <*slot/port*>	Optional. Activates debug messages for the client using the specified gigabit switchport interface.
interface switchport <*slot/port*>	Optional. Activates debug messages for the client using the specified switchport interface.
interface xgigabit-switchport <*slot/port*>	Optional. Activates debug messages for the client using the specified 10 gigabit switchport interface.
ip <*ip address*>	Optional. Activates debug messages for the client with the specified IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
mac <*mac address*>	Optional. Activates debug messages for the client with the specified medium access control (MAC) address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release 17.8	Command was introduced.
Release R10.7.0	Command was expanded to include the switchport and 10 gigabit switchport interfaces.

Usage Examples

The following is sample output of the **debug network-forensics ip dhcp** command:

>**enable**
#debug network-forensics ip dhcp
2009.08.31 14:30:30 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/5 Discover from 00:E0:29:0E:D5:E3 (xpsp3-host)
2009.08.31 14:30:31 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/24 Offer from 00:E0:29:0E:D5:E5/10.23.220.254 to 00:E0:29:0E:D5:E3 of 10.23.220.1/255.255.255.0(xpsp3-host)
2009.08.31 14:30:31 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/5 Request from 00:E0:29:0E:D5:E3 10.23.220.1/255.255.255.0 (xpsp3-host) to 00:E0:29:0E:D5:E5/10.23.220.254
2009.08.31 14:30:31 NETWORK_FORENSICS.IP.DHCP.giga-swx 0/24 Ack from 00:E0:29:0E:D5:E5/10.23.220.254 to 00:E0:29:0E:D5:E3 of 10.23.220.1/255.255.255.0 (xpsp3-host)

debug network-sync

Use the **debug network-sync** command to enable debug messaging for network synchronization (Network Sync). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug network-sync clock
debug network-sync clock defects
debug network-sync clock status
debug network-sync ssm
debug network-sync ssm rx
debug network-sync ssm tx
debug network-sync ssm events
debug network-sync ssm events rx
debug network-sync ssm events tx

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

clock	Specifies Network Sync clock debug messages are enabled.
defects	Optional. Specifies that debug messages for Network Sync clock defect events are enabled.
status	Optional. Specifies that debug messages for Network Sync clock status events are enabled.
ssm	Specifies that debug messages for Network Sync synchronization status messages (SSMs) are enabled.
events	Optional. Specifies that debug message for SSM events are enabled.
rx	Optional. Specifies that debug messages for received SSM events are enabled.
tx	Optional. Specifies that debug messages for transmitted SSM events are enabled.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example enables debug messages for Network Sync clock events:

>**enable**
#debug network-sync clock

The following example enables debug messages for Network Sync SSM events:

>**enable**
#debug network-sync ssm events

debug nslookup

Use the **debug nslookup** command to activate debug messages associated with name server lookup client (nslookup) events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R13.3.0	Command was introduced.

Usage Examples

The following example activates debug messages associated with nslookup events:

```
>enable
#debug nslookup
```


debug ntp

Use the **debug ntp** command to activate debug messages associated with the Network Time Protocol (NTP) daemon information. Adding the virtual routing and forwarding (VRF) name to this command displays debug information only for the named VRF. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug ntp
debug ntp any-vrf
debug ntp vrf <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

any-vrf	Optional. Displays debug information for all VRF instances, including the default.
vrf <*name*>	Optional. Displays debug information for the specified VRF instance.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.2	Command was introduced.
Release R10.7.0	Command was expanded to include the **vrf** and **any-vrf** parameters.

Usage Examples

The following example activates debug messages associated with NTP:

>enable
#debug ntp

debug ospfv3

Use the **debug ospfv3** command to activate debug messages associated with Open Shortest Path First version 3 (OSPFv3). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ospfv3
debug ospfv3 adj
debug ospfv3 adj errors
debug ospfv3 database-timer
debug ospfv3 events
debug ospfv3 flood
debug ospfv3 flood errors
debug ospfv3 hello
debug ospfv3 hello errors
debug ospfv3 lsa-generation
debug ospfv3 packet errors
debug ospfv3 packet rx
debug ospfv3 packet rx summary
debug ospfv3 packet tx
debug ospfv3 packet tx summary
debug ospfv3 retransmission
debug ospfv3 spf
debug ospfv3 spf router-calculation
debug ospfv3 <*process id*>
debug ospfv3 <*process id*> **adj**
debug ospfv3 <*process id*> **adj errors**
debug ospfv3 <*process id*> **database-timer**
debug ospfv3 <*process id*> **events**
debug ospfv3 <*process id*> **flood**
debug ospfv3 <*process id*> **flood errors**
debug ospfv3 <*process id*> **hello**
debug ospfv3 <*process id*> **hello errors**
debug ospfv3 <*process id*> **lsa-generation**
debug ospfv3 <*process id*> **packet errors**
debug ospfv3 <*process id*> **packet rx**
debug ospfv3 <*process id*> **packet rx summary**
debug ospfv3 <*process id*> **packet tx**
debug ospfv3 <*process id*> **packet tx summary**
debug ospfv3 <*process id*> **retransmission**
debug ospfv3 <*process id*> **spf**
debug ospfv3 <*process id*> **spf router-calculation**

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<process id>	Optional. Displays debug information for the specified OSPFv3 routing process. If no process ID is specified, information for all OSPFv3 processes is displayed. Valid process ID range is **1** to **65535**.
adj	Specifies that only OSPFv3 adjacency events are displayed.
database-timer	Specifies that only OSPFv3 database timer information is displayed.
events	Specifies that only OSPFv3 events are displayed.
errors	Optional. Specifies that errors about specific information are displayed.
flood	Specifies that only OSPFv3 flooding information is displayed.
hello	Specifies that only OSPFv3 Hello events are displayed.
lsa-generation	Specifies that only OSPFv3 link state advertisement (LSA) generation information is displayed.
packet errors	Specifies that only OSPFv3 errors with received packets are displayed.
packet rx	Specifies that only OSPFv3 received packet information is displayed.
packet tx	Specifies that only OSPFv3 transmitted packet information is displayed.
summary	Optional. Summarizes OSPFv3 packet information.
retransmission	Specifies that only OSPFv3 retransmission events are displayed.
spf	Specifies that OSPFv3 shortest path first (SPF) events are displayed.
spf route-calculation	Specifies that OSPFv3 SPF route calculations are displayed.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example activates the debug messages for all OSPFv3 processes on the AOS device:

```
>enable
#debug ospfv3
Receiving OSPFv3 packet from 2001:db8:10:24::106.4 to FF02::5 on eth 0/1.6
    SysUpTime=1222577915 ms.
    Hello Packet from Router ID: 1.1.1.4; Ver:2 Length:48
    Area ID: 0.0.0.0 Checksum: )x8659;; Using Null Authentication: 0:0
    PrefixLenV4: /64; Hello Interval: 10 Options: 0x13 Router Priority: 1 Router Dead Interval: 40
    Designated Router: 10.24.106.4 Backup Designated Router: 10.24.106.5
    1 Neighbors:
        123.1.1.1
16:35:24: OSPFv3: HELLO received form 1.1.1.4, neighbor state is FULL
```

debug over-temperature protection

Use the **debug over-temperature protection** command to activate debug messages associated with over-temperature protection events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug over-temperature protection
debug over-temperature protection sensor
debug over-temperature protection voting

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

sensor	Optional. Displays debug messages only for the over-temperature protection temperature sensor.
voting	Optional. Displays debug messages only for the over-temperature protection temperature voting events.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example activates debug messages for the over-temperature protection feature:

>enable
#debug over-temperature protection

debug packet-capture

Use the **debug packet-capture** command to enable debug messaging for all packet-capture activities. Use the **no** form of this command to disable packet-capture debug messaging.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example enables debug messaging for all packet-capture activities:

```
>enable
#debug packet-capture
```

debug ping twamp

Use the **debug ping twamp** command to activate debug messages associated with Two-Way Active Measurement Protocol (TWAMP) ping activity. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ping twamp
debug ping twamp control
debug ping twamp control events
debug ping twamp control packets
debug ping twamp test
debug ping twamp test events
debug ping twamp test packets

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

control		Optional. Activates TWAMP control debug messages.
	events	Optional. Displays TWAMP control events and messages.
	packets	Optional. Displays TWAMP control events and packets.
test		Activates TWAMP Test debug messages.
	events	Optional. Displays TWAMP test events and messages.
	packets	Optional. Displays TWAMP test events and packets.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.6	Command was introduced.

Usage Examples

The following example enables debug messaging for TWAMP control events and messages:

>enable
#debug ping twamp control
Type CTRL+C to abort. Test will complete in approximately 7 seconds.

2009.06.03 11:18:51 IP.TWPING CTRL EVNT Attempting to connect
2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Init -> Opening (event=Open Connection)
2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Opening -> Setup (event=RX


```
    Server-Greeting)
2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Setup -> Starting (event=TX
    Setup-Response)
2009.06.03 11:18:51 IP.TWPING CTRL PKT Sending Setup-Response (len=140)
 mode=1
 keyId=00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

 token=00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Starting -> Active (event=RX Server-Start)
2009.06.03 11:18:51 IP.TWPING CTRL PKT Received Server-Start (len=48)
 accept=0 serverIV=3d97e36d000000000178343030386337 startTime=4a26a1ad.2be49403
2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Active -> Register-Session (event=TX
    Request-Session)
2009.06.03 11:18:51 IP.TWPING CTRL PKT Sending Request-Session (len=112)
 ipVer=4 confSender=0 confReceiver=0 numSchedSlots=0 numPkts=10
 senderPort=1090 receiverPort=0 senderIp=10.22.135.18 receiverIp=10.22.130.44
 sessId=00000000000000000000000000000000 padLen=0
 startTime=0.0 timeout=2.0 dscp=0
2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Register-Session -> Active (event=RX
    Accept-Session)
2009.06.03 11:18:51 IP.TWPING CTRL PKT Received Accept-Session (len=48)
 accept=0 port=1063 sessId=0000000000000025cf198506ac7bb859
2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Active -> Start-Sessions (event=TX
    Start-Sessions)
2009.06.03 11:18:51 IP.TWPING CTRL PKT Sending Start-Sessions (len=32)

2009.06.03 11:18:51 IP.TWPING CTRL EVNT State changed Start-Sessions -> Active (event=RX
    Start-Ack)
2009.06.03 11:18:51 IP.TWPING CTRL PKT Received Start-Ack (len=32)
 accept=0--- statistics from [10.22.135.18]:1090 to [10.22.130.44]:1063

SID: 00000003720725133617212318489
10 sent, 0 lost (0.000%)

Delay
 round-trip  min/avg/max  =        0        0          0 ms
             num/sum/sum2 =       10        9          9 ms
 out         min/avg/max  =       -6       -6         -6 ms
             num/sum/sum2 =       10      -62        388 ms
 in          min/avg/max  =        7        7          7 ms
             num/sum/sum2 =       10       72        522 ms
```

```
IPDV-abs
  round-trip   min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          9        0                0 ms
  out          min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          9        0                0 ms
  in           min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          9        0                0 ms
IPDV-pos
  round-trip   min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          4        0                0 ms
  out          min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          2        0                0 ms
  in           min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          7        0                0 ms
IPDV-neg
  round-trip   min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          5        0                0 ms
  out          min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          7        0                0 ms
  in           min/avg/max  =          0        0                0 ms
               num/sum/sum2 =          2        0                0 ms
clock error
    local  =     sync, 0.488281 ms
    remote =     sync, 0.488281 ms

2009.06.03 11:18:53 IP.TWPING CTRL EVNT State changed Active -> Stop-Sessions (event=TX
     Stop-Session)
2009.06.03 11:18:53 IP.TWPING CTRL PKT Sending Stop-Sessions (len=32)
  accept=0 numSessions=0
2009.06.03 11:18:53 IP.TWPING CTRL EVNT State changed Stop-Sessions -> Active (event=Stopping
     Tests)
2009.06.03 11:18:53 IP.TWPING CTRL EVNT Closing connection
2009.06.03 11:18:53 IP.TWPING CTRL EVNT State changed Active -> Closed (event=Close Connection)
```

debug port-auth

Use the **debug port-auth** command to generate debug messages used to aid in troubleshooting problems during the port authentication process. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug port-auth
debug port-auth auth-sm
debug port-auth bkend-sm
debug port-auth general
debug port-auth packet
debug port-auth packet [both | tx | rx]
debug port-auth reauth-sm
debug port-auth supp-sm
debug port-auth voice

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

auth-sm	Optional. Displays AuthPAE-state machine information.
bkend-sm	Optional. Displays backend-state machine information.
general	Optional. Displays configuration changes to the port authentication system.
packet both	Optional. Displays packet exchange information in both receive and transmit directions.
packet rx	Optional. Displays packet exchange information in the receive-only direction.
packet tx	Optional. Displays packet exchange information in the transmit-only direction.
reauth-sm	Optional. Displays reauthentication-state machine information.
supp-sm	Optional. Displays supplicant-state machine information.
voice	Optional. Displays voice-based port authentication information.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.1	Command was introduced.
Release 10.1	New options were introduced.
Release 13.1	New options were introduced.
Release R11.13.0	Command was expanded to include the **voice** parameter.

Usage Examples

The following example activates port authentication debug information on received packets:

>**enable**
#debug port-auth packet rx
Rcvd EAPOL Start for sess 1 on int eth 0/2

debug port security

Use the **debug port security** command to display messages associated with port security. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates port security debug messages:

```
>enable
#debug port security
```

debug ppp

Use the **debug ppp** command to activate debug messages associated with Point-to-Point Protocol (PPP) operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ppp authentication
debug ppp errors
debug ppp negotiation
debug ppp verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

authentication	Activates debug messages pertaining to PPP authentication (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), Extensible Authentication Protocol (EAP), etc.).
errors	Activates debug messages that indicate a PPP error was detected (mismatch in negotiation authentication, etc.).
negotiation	Activates debug messages associated with PPP negotiation.
verbose	Activates detailed debug messages for PPP operation.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **debug ppp** command activates debug messages to provide information on PPP activity in the system. PPP debug messages can be used to aid in troubleshooting PPP links.

Usage Examples

The following example activates debug messages associated with PPP authentication activity:

>enable
#debug ppp authentication

debug pppoe client

Use the **debug pppoe client** command to activate debug messages associated with Point-to-Point Protocol over Ethernet (PPPoE) operation in AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with PPPoE activity:

```
>enable
#debug pppoe client
```

debug probe

Use the **debug probe** command to activate debug messages associated with activities performed by the named probe object. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug probe
debug probe <*name*>
debug probe <*name*> **twamp**
debug probe <*name*> **twamp control**
debug probe <*name*> **twamp control events**
debug probe <*name*> **twamp control packets**
debug probe <*name*> **twamp test**
debug probe <*name*> **twamp test events**
debug probe <*name*> **twamp test packets**

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*name*>	Optional. Specifies the probe object or activates the probe database debug event messages for the specified probe.
twamp	Optional. Specifies Two-Way Active Measurement Protocol (TWAMP) probe verbose output.
control	Activates TWAMP control probe verbose messages.
events	Optional. Activates TWAMP control probe events.
packets	Optional. Activates decode TWAMP control packets messages.
test	Activates TWAMP Test probe verbose output.
events	Optional. Activates TWAMP Test probe events.
packets	Optional. Activates decode TWAMP Test packets messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.
Release 17.3	Command was expanded to include the TWAMP probe verbose output.

Usage Examples

The following example activates all debug messages associated with the probes:

>**enable**
#debug probe

The following example activates debug messages associated with the probe object named **probe_A**:

>**enable**
#debug probe probe_A

debug probe responder

Use the **debug probe responder** command to display probe responder event messages or activate debug messages associated with activities performed by the named probe object. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug probe responder twamp
debug probe responder twamp control
debug probe responder twamp control event
debug probe responder twamp control event <*address*>
debug probe responder twamp control packet
debug probe responder twamp control packet <*address*>
debug probe responder twamp test
debug probe responder twamp test event
debug probe responder twamp test event <*address*>
debug probe responder twamp test packet
debug probe responder twamp test packet <*address*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

twamp	Optional. Activates probe debug messages for all Two-Way Active Measurement Protocol (TWAMP) responder verbose output.
control	Optional. Activates probe debug messages for TWAMP control responder verbose output.
event <*address*>	Optional. Activates probe debug messages for TWAMP control responder events. Specify the far-end IP address to activate remote events.
packet <*address*>	Optional. Activates probe debug messages to decode TWAMP control packets. Enter an IP address to decode TWAMP control packets from a specific address.
test	Optional. Activates probe debug messages for TWAMP test responder verbose output.
event <*address*>	Optional. Activates probe debug messages for TWAMP test responder events. Enter a far-end IP address to display events from the specified address.
packet <*address*>	Optional. Activates probe debug messages to decode TWAMP test packets. Enter an IP address to decode TWAMP test packets from a specific address.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 13.1	Command was introduced.
Release 17.2	Command was expanded to include the TWAMP responder debug options.

Usage Examples

The following example activates debug messages associated with all probe objects:

>**enable**
#debug probe

The following example activates debug messages associated with the probe object named **probe_A**:

>**enable**
#debug probe probe_A

The following example activates probe responder debug messages:

>**enable**
#debug probe responder

debug radius

Use the **debug radius** command to enable debug messages from the remote authentication dial-in user service (RADIUS) subsystem. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The **debug radius** messages show the communication process with the remote RADIUS servers.

Usage Examples

The following is sample output for the **debug radius** command:

```
>enable
#debug radius
RADIUS AUTHENTICATION: Sending packet to 172.22.48.1 (1645).
RADIUS AUTHENTICATION: Received response from 172.22.48.1.
```


debug restore

Use the **debug restore** command to restore the last saved debug filters to the unit.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.4	Command was introduced.

Functional Notes

This command is used to restore filters saved using the command *debug save on page 450*. To view the saved filters without restoring them to the unit, use the **show debugging saved-filters** command (refer to *show debugging on page 594*).

Usage Examples

The following example restores previously saved debug filters on the AOS unit:

```
>enable
#debug restore
Restoring saved debug filters...
Filters to restore:
debug mail-client agent
debug probe test1
Running restoration script...done
```


debug rtp media

Use the **debug rtp media** command to display media event debug messages (real time) to the terminal (or Telnet) screen. Debug messages are generated for media functions, such as the beginning and ending of anchoring sessions and the creation and destruction of associations. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.8.0	Command was introduced.

Usage Examples

The following example activates RTP packets debug messages for media events:

>enable
#debug rtp media

debug rtp quality-monitoring

Use the **debug rtp quality-monitoring** command to display voice quality monitoring (VQM) event debug messages (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug rtp quality-monitoring
debug rtp quality-monitoring packets
debug rtp quality-monitoring packets rtcp
debug rtp quality-monitoring packets rtp
debug rtp quality-monitoring packets round-trip-delay

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

packets	Optional. Displays VQM debug events of voice traffic packets.
rtcp	Optional. Displays VQM debug messages for Realtime Transport Control Protocol (RTCP) packet events.
rtp	Optional. Displays VQM debug messages for Realtime Transport Protocol (RTP) packet events.
round-trip-delay	Optional. Displays VQM debug messages for round-trip delay mechanism events.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.1	Command was introduced.
Release A1	Command was included in the AOS voice products.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example activates RTP packets debug messages for VQM:

```
>enable
#debug rtp quality-monitoring packets rtp
2007.10.23 17:35:06 VQM.PACKET RTCP   Sender SSRC=1244609021
2007.10.23 17:35:06 VQM.PACKET RTCP   NTP timestamp (MSW)=3402167683 (0xcac8f583)
2007.10.23 17:35:06 VQM.PACKET RTCP   NTP timestamp (LSW)=1116355952 (0x428a3d70)
2007.10.23 17:35:06 VQM.PACKET RTCP   RTP timestamp=3990799999
2007.10.23 17:35:06 VQM.PACKET RTCP   SSRC=1919245558
```



```
2007.10.23 17:35:06 VQM.PACKET RTCP   Last SR timestamp=4119950126 (0xf591732e)
2007.10.23 17:35:06 VQM.PACKET RTCP   Delay since last SR timestamp=175671
2007.10.23 17:35:06 VQM.PACKET RTCP   handle=0x6179810ebu
2007.10.23 17:35:09 VQM.PACKET RTCP Rx RTCP SR pkt from 10.22.41.91
2007.10.23 17:35:09 VQM.PACKET RTCP   call-ID=30bbb408417e519a00be27ac15d5776b@1
    0.22.41.52
2007.10.23 17:35:09 VQM.PACKET RTCP   Sender SSRC=1919245558
2007.10.23 17:35:09 VQM.PACKET RTCP   NTP timestamp (MSW)=3402167702 (0xcac8f596)
2007.10.23 17:35:09 VQM.PACKET RTCP   NTP timestamp (LSW)=1932399624 (0x732e1408)
2007.10.23 17:35:09 VQM.PACKET RTCP   RTP timestamp=2621875150
2007.10.23 17:35:09 VQM.PACKET RTCP   SSRC=1244609021
2007.10.23 17:35:09 VQM.PACKET RTCP   Last SR timestamp=4119020170 (0xf583428a)
2007.10.23 17:35:09 VQM.PACKET RTCP   Delay since last SR timestamp=151436
2007.10.23 17:35:09 VQM.PACKET RTCP   handle=0x6524010g all
```


debug rtp quality-monitoring reporter

Use the **debug rtp quality-monitoring reporter** to activate debug messages associated with voice quality monitoring (VQM) reporters. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug rtp quality-monitoring reporter
debug rtp quality-monitoring reporter <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*name*>	Optional. Specifies that debug messages are enabled only for the named reporter.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.6	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following is sample output of debug messages for VQM reporter **Reporter1**:

>enable
#debug rtp quality-monitoring reporter Reporter1
08:46:13 VQM.REPORTER Reporter1 1 Enqueuing VQM Report - 2575556352@10.1.3.9 to 6353@10.1.3.9, RTP=10.10.20.2:2234->10.17.138.1:3000
08:46:13 VQM.REPORTER Reporter1 1 Generating VQM Report
08:46:13 VQM.REPORTER Reporter1 1 Sending VQM Report
08:46:13 VQM.REPORTER Reporter1 1 Transaction 0x022ad5f0: state changed -> Client General Request Sent

debug save

Use the **debug save** command to perform a persistent save of the debug filters enabled in the current command line interface (CLI) session. The saved filters can be restored at a later time.

> NOTE *Turning on a large amount of debug information can adversely affect the performance of your unit.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.4	Command was introduced.

Functional Notes

This command is used to save debug filters across a unit reboot. Filters are restored using the command *debug restore on page 445*. To view the saved filters without restoring them to the unit, use the **show debugging saved-filters** command (refer to *show debugging on page 594*).

Only one set of filters can be saved per instance of AOS. If a previous set of filters has been saved, issuing the **debug save** command overwrites the previously saved filters with the current set of filters. If no filters are currently active, issuing **debug save** has no effect so that the last saved files are not lost.

Usage Examples

The following example saves the debug filters from the current CLI session:

```
>enable
#debug save
Saving debug filters enabled in this session...
debug mail-client agent
debug probe test1
Done.
```


debug schedule

Use the **debug schedule** command to activate debug messages associated with a schedule. Variations of this command include:

debug schedule
debug schedule <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*name*>	Optional. Displays only the debug information for a specific schedule.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example enables debug information for any configured schedules:

>**enable**
#debug schedule
01:00:15: NETMON.SCHEDULE MIDNIGHT: status changed to inactive

debug sip

Use the **debug sip** command to activate debug messages associated with Session Initiation Protocol (SIP) events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug sip cldu
debug sip location
debug sip manager
debug sip name-service
debug sip secure remote-user
debug sip syntax
debug sip tdu
debug sip trunk-registration
debug sip trunk-registration <*Txx*>
debug sip trunk-registration <*Txx*> <*trunk id*>
debug sip user-registration
debug sip user-registration <*extension*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

cldu	Activates SIP call leg distribution unit (CLDU) event debug messages.
location	Activates SIP location database event debug messages.
manager	Activates SIP stack manager event debug messages.
name-service	Activates SIP name-service event debug messages.
secure remote-user	Activates SIP security remote user debug messages.
syntax	Activates SIP syntax event debug messages.
tdu	Activates SIP transaction distribution unit (TDU) debug messages.
trunk-registration	Activates all SIP trunk-registration event debug messages.
trunk-registration <*Txx*>	Optional. Activates SIP trunk-registration event debug messages for a specific trunk. For example: Txx (T01) where xx is the trunk's two-digit identifier.
trunk-registration <*Txx*> <*trunk id*>	Optional. Activates SIP trunk-registration event debug messages for a specific trunk. For example: Txx (T01) where xx is the trunk's two-digit identifier and <trunk id> is the specific name associated with the trunk.
user-registration	Activates all SIP user-registration event debug messages.
user-registration <*extension*>	Optional. Activates SIP user-registration event debug messages for a specific trunk.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the proxy event messages.
Release 15.1	Command was expanded to include the name-service messages.
Release 16.1	Command was expanded to include the TDU messages.
Release 17.3	Command was expanded to include the syntax messages.
Release R10.7.0	Command was expanded to include the **secure remote-user** parameter.

Usage Examples

The following example activates all debug messages associated with SIP CLDU events:

```
>enable
#debug sip cldu
```

debug sip connections

Use the **debug sip connections** command to activate debug messages associated with setting up and tearing down a Session Initiation Protocol (SIP) connection to remote peer. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug sip connections
debug sip connections persistence

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

persistence	Activates SIP connection debug messages only for persistent connections.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example activates all debug messages associated with SIP connection events:

>enable
#debug sip connections

debug sip proxy

Use the **debug sip proxy** command to activate debug messages associated with Session Initiation Protocol (SIP) proxy events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug sip proxy database
debug sip proxy database verbose
debug sip proxy dialogs
debug sip proxy register rate-adaption
debug sip proxy routing
debug sip proxy transactions
debug sip proxy verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

database	Activates SIP proxy database debug event debug messages.
verbose	Activates more detailed debug messages concerning SIP proxy user database lookups.
dialogs	Activates SIP proxy DOM event debug messages.
register rate-adaption	Activates SIP proxy REGISTER rate adaption debug messages.
routing	Activates SIP proxy message-routing events.
transactions	Activates SIP proxy event debug messages that shows the interaction between the SIP proxy and the SIP stack.
verbose	Activates all SIP proxy debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.
Release A5.02	Command was expanded to include the **register rate-adaption** parameter.
Release R11.10.5	Command was expanded to include the **verbose** option for **debug sip proxy database**.

Usage Examples

The following example activates all debug messages associated with SIP proxy events:

>**enable**
#debug sip proxy verbose

debug sip stack

Use the **debug sip stack** command to activate debug messages associated with Session Initiation Protocol (SIP) stack events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug sip stack debug
debug sip stack errors
debug sip stack exceptions
debug sip stack info
debug sip stack messages [**ack** | **all** | **bye** | **cancel** | **info** | **invite** | **message** | **notify** | **options** | **prack** | **publish | refer | register | request | response | subscribe | update] [from** <*user*> | **request** | **response** | **rx** | **to** <*user*> | **tx**]
debug sip stack messages [**from** <*user*> | **request** | **response** | **rx** | **to** <*user*> | **tx**]
debug sip stack messages summary [**ack** | **all** | **bye** | **cancel** | **info** | **invite** | **message** | **notify** | **options** | **prack** | **publish** | **refer** | **register** | **request** | **response** | **subscribe** | **update**] [**from** <*user*> | **request** | **response** | **rx** | **to** <*user*> | **tx**]
debug sip stack verbose
debug sip stack warnings

Turning on a large amount of debug information can adversely affect the performance of your unit.

*The majority of the **debug sip stack messages** variations are available in any order, at any time within the subcommand. Use the **?** at any level after each variation listed within the brackets to view additional arguments and variations for the subcommand(s).*

Syntax Description

debug	Activates SIP stack debug event debug messages.
errors	Activates SIP stack error event debug messages.
exceptions	Activates SIP stack exception event debug messages.
info	Activates SIP stack info event debug messages.
messages	Specify which SIP debug messages to activate from the list below.
ack	Activates SIP ACK debug messages.
all	Activates all SIP debug messages.
bye	Activates SIP BYE debug messages.
cancel	Activates SIP CANCEL debug messages.
from <*user*>	Activates SIP debug messages from the specified user.
info	Activates SIP INFO debug messages.
invite	Activates SIP INVITE debug messages.
message	Activates SIP MESSAGES debug messages.

notify	Activates SIP NOTIFY debug messages.
options	Activates SIP OPTIONS debug messages.
prack	Activates SIP PRACK debug messages.
publish	Activates SIP PUBLISH debug messages.
refer	Activates SIP REFER debug messages.
register	Activates SIP REGISTER debug messages.
request	Activates the specified SIP request debug messages.
response	Activates the specified SIP response debug messages.
rx	Activates received SIP debug messages **to** or **from** a specific user.
subscribe	Activates SIP SUBSCRIBE debug messages.
summary	Activates SIP debug messages and displays only a summary (first line) of the available messages.
to <*user*>	Activates SIP debug messages to the specified user.
tx	Activates transmitted SIP debug messages **to** or **from** a specific user.
update	Activates SIP UPDATE debug messages.
verbose	Activates all SIP stack event debug messages.
warnings	Activates SIP stack warning event debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.3	Command was introduced.
Release A1	Command was expanded in the AOS voice products.

Usage Examples

The following example activates all debug messages associated with SIP stack events:

```
>enable
#debug sip stack all
```

debug snmp packets

Use the **debug snmp packets** command to enable debug output from local Simple Network Management Protocol (SNMP) traffic. Debug messages are displayed (real time) to the terminal (or Telnet) screen. When SNMP packets ingress or egress the unit (local traffic only), the traffic is displayed in a partially decoded form. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following is an example of debug output for snmp packets:

```
>enable
#debug snmp packets
#SNMP V1 RX: GET-NEXT Request PDU from 10.23.1.157:2922 (community=public)
 request id=3, error status=0, error index=0
 max repetitions=0, non repetitions=0
 VarBinds:
   OID=1.3.6.1.2.1.1.3
   value=empty

#SNMP V1 TX: GET Response PDU to 10.23.1.157:2922 (community=public)
 request id=3, error status=0, error index=0
 max repetitions=1, non repetitions=0
 VarBinds:
   OID=1.3.6.1.2.1.1.3.0
   value=410825
```


debug sntp

Use the **debug sntp** command to enable debug messages associated with the Simple Network Time Protocol (SNTP). All SNTP packet exchanges and time decisions are displayed with these debugging events enabled. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug sntp client
debug sntp server

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

client	Displays SNTP client information.
server	Displays SNTP server information.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 3.1	Command was introduced.
Release 13.1	Command was expanded to include the client and server options.

Functional Notes

The **debug sntp** command activates debug messages to aid in troubleshooting SNTP issues.

Usage Examples

The following is sample output for the **debug sntp client** command:

>enable
#debug sntp client
#configure terminal
#sntp server ntp.adtran.com
2009.03.16 15:38:06 SNTP.CLIENT sent Version 1 SNTP time request to 172.22.48.13
2009.03.16 15:38:06 SNTP.CLIENT received SNTP reply packet from 172.22.48.13
2009.03.16 15:38:06 SNTP.CLIENT setting time to 03-16-2009 15:37:54 CDT
2009.03.16 15:37:54 SNTP.CLIENT waiting for 86400 seconds for the next poll interval

debug spanning-tree

Use the **debug spanning-tree** command to enable the display of spanning-tree debug messages. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug spanning-tree config
debug spanning-tree events
debug spanning-tree general
debug spanning-tree topology

Turning on a large amount of debug information can adversely affect the performance of your unit.

Refer to debug spanning-tree bpdu on page 462 for more information.

Syntax Description

config	Enables the display of spanning-tree debug messages when configuration changes occur.
events	Enables the display of debug messages when spanning-tree protocol events occur.
general	Enables the display of general spanning-tree debug messages.
topology	Enables the display of debug messages when spanning-tree protocol topology events occur.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 5.1	Command was introduced.
Release 12.1	Command was expanded to include **topology**.

Usage Examples

The following example enables the display of general spanning-tree debug messages:

```
>enable
#debug spanning-tree general
```


debug spanning-tree bpdu

Use the **debug spanning-tree bpdu** command to display bridge protocol data unit (BPDU) debug messages. When enabled, a debug message is displayed for each BPDU packet that is transmitted or received by the unit. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug spanning-tree bpdu all
debug spanning-tree bpdu receive
debug spanning-tree bpdu transmit

Turning on a large amount of debug information can adversely affect the performance of your unit.

Refer to debug spanning-tree on page 461 for more information.

Syntax Description

all	Displays debug messages for BPDU packets that are transmitted and received by the unit.
receive	Displays debug messages for BPDU packets received by the unit.
transmit	Displays debug messages for BPDU packets transmitted by the unit.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example displays debug messages for BPDU packets that are transmitted and received by the unit:

```
>enable
#debug spanning-tree bpdu all
```


debug ssh

Use the **debug ssh** command to activate debug messages associated with secure shell (SSH) client and server information. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug ssh client events
debug ssh client port-forward
debug ssh client scp
debug ssh client sftp
debug ssh server events

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

client events	Enables the display of SSH client events.
client port-forward	Enables the display of SSH port forward information.
client scp	Enables the display of SSH client SCP information.
client sftp	Enables the display of SSH client SFTP information.
server events	Enables the display of SSH and SCP server events.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.10.0	Command was introduced.
Release R11.4.0	Command was expanded to include the **client port-forward** parameter.
Release R13.11.0	Command was expanded to include the **client sftp** parameter.

Usage Examples

The following enables the display of SSH server event debug messages:

>enable
#debug ssh server events

debug stack

Use the **debug stack** command to enable switch-stacking debug messages. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.Variations of this command include:

debug stack
debug stack switch
debug stack verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

switch	Optional. Enables messages specific to the stack ports (stack switch application program interface (API) information).
verbose	Optional. Enables detailed messages specific to the stack protocol.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates the possible debug stack messages:

>enable
#debug stack switch
#debug stack verbose

debug system

Use the **debug system** command to enable debug messages associated with system events (i.e., login, logouts, etc.). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with system information:

```
>enable
#debug system
```

debug tacacs+

Use the **debug tacacs+** command to activate debug messages associated with terminal access controller access-control system plus (TACACS+) protocol. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug tacacs+
debug tacacs+ events
debug tacacs+ packets

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

events	Optional. Activates TACACS+ event debug messages.
packets	Optional. Activates TACACS+ packet debug messages.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with the TACACS+ protocol:

```
>enable
#debug tacacs+ packets
```


debug tcl

Use the **debug tcl** command to activate debug messages associated with tool command language (Tcl) interpreter operation. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug tcl cli
debug tcl cli <*filename*>
debug tcl track <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

cli	Displays debug messages for the Tcl interpreter to the command line interface (CLI).
<*filename*>	Optional. Displays debug messages only for the specified Tcl script file.
track <*name*>	Displays debug messages for the specified track. The **track** parameter is only available on platforms with Network Monitoring enabled.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example activates debug messages for the Tcl interpreter while running the file **test1.tcl**:

>**enable**
#debug tcl test1.tcl

debug tls sip

Use the **debug tls sip** command to enable debug messages for Session Initiation Protocol (SIP) Transport Layer Security (TLS) functionality. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug tls sip events
debug tls sip negotiation

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

events	Displays TLS events, such as errors and state changes.
negotiation	Displays information about each step of all TLS handshakes.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example enables debug messages for all SIP TLS events:

```
>enable
#debug tls sip
```


debug track

Use the **debug track** command to activate debug messages associated with activities performed by track objects. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include:

debug track
debug track <*name*>

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<*name*>	Optional. Displays information about the specified track rather than all configured tracks.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with all track objects:

>enable
#debug track

The following example activates debug messages associated with the track object named **track_1**:

>enable
#debug track track_1

debug voice

Use the **debug voice** command to activate debug messages associated with voice functionality. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug voice account-status
debug voice conference local
debug voice dsp
debug voice dsp voip <*slot/port*> **channel** <*number*> **ecan**
debug voice dsp voip <*slot/port*> **channel** <*number*> **rfc2833**
debug voice dsp voip <*slot/port*> **channel** <*number*> **rtp**
debug voice dsp voip <*slot/port*> **channel verbose rfc2833**
debug voice dsp voip <*slot/port*> **channel verbose rtp**
debug voice erltool
debug voice erltool info
debug voice erltool statemachine
debug voice lineaccount
debug voice lineaccount <*line*>
debug voice linemanager
debug voice linemanager <*line*>
debug voice loopback
debug voice phonemanager
debug voice phonemanager <*slot:port*>
debug voice ring-group
debug voice ring-group <*group*>
debug voice rtp channel
debug voice rtp conference local
debug voice rtp manager
debug voice rtp provider
debug voice rtp verbose
debug voice smdr
debug voice smdr <*number*>
debug voice srtp
debug voice srtp sdes
debug voice srtp sdes events
debug voice srtp sdes negotiation
debug voice srtp sdes parse
debug voice stationaccount
debug voice stationaccount <*extension*>
debug voice summary
debug voice switchboard
debug voice switchboard <*subsource*>
debug voice switchboard call
debug voice switchboard call <*call id*>
debug voice switchboard ccm

debug voice toneservices
debug voice toneservices *<notifies>*
debug voice toneservices *<interface>*
debug voice toneservices *<interface> <slot/port>*
debug voice trunkaccount
debug voice trunkaccount *<trunk id>*
debug voice trunkaccount *<trunk id> <appearance>*
debug voice trunkmanager
debug voice trunkmanager *<trunk id>*
debug voice trunkmanager *<trunk id> <appearance>*
debug voice trunkport
debug voice trunkport *<slot:port:DS0>*
debug voice verbose

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

account-status	Activates station account status event debug messages.
dsp	Activates digital signal processor (DSP) event debug messages.
voip *<slot/port>* **channel**	Optional. Activates DSP on the specified interface and DSP channel.
<number>	Optional. Activates DSP on the specified interface and DSP channel.
ecan	Optional. Activates the echo canceller debug feature.
rfc2833	Optional. Activates the RFC 2833 debug feature.
rtp	Optional. Activates Realtime Transfer Protocol (RTP) event debug messages for the specified interface and channel.
verbose	Optional. Activates detailed debug DSP messaging for the RTP and RFC 2833 features.
erltool	Activates the echo return loss (ERL) debug messages to monitor the progress of the testing.
info	Optional. Activates information events related to the ERL tool testing progress.
statemachine	Optional. Activates ERL tool state machine events.
lineaccount	*Activates all line account event debug messages.*
<line>	Optional. *Activates a specific line account event debug messages.*
linemanager	*Activates all line manager event debug messages.*
<line>	Optional. *Activates a specific line manager event debug messages.*
loopback	*Activates all voice loopback account event debug messages.*
phonemanager	Activates all phone manager event debug messages.
<slot:port>	Optional. Activates phone manager event debug messages for a specific slot and port.

ring-group	Activates ring-group event debug messages.
<group>	Optional. Activates event debug messages for a specified group.
rtp	Activates Realtime Transport Protocol (RTP) event debug messages.
channel	Activates RTP channel event debug messages.
conference local	Activates local conference session debug messages.
manager	Activates RTP manager event debug messages.
provider	Activates RTP provider event debug messages.
verbose	Activates detailed RTP debug messages.
smdr	Activates all station message detail reporting (SMDR) event debug messages.
<number>	Optional. Activates SMDR event debug messages for a specific to or from number.
srtp	Activates debug messages for Secure Realtime Transfer Protocol (SRTP).
sdes	Optional. Activates debug messages for Session Description Protocol Security Descriptions (SDES) key management of SRTP.
events	Optional. Displays SDES events, such as errors and state changes.
negotiation	Optional. Displays information about each step of all SDES negotiations.
parse	Optional. Displays information about the parsing of SDES content.
stationaccount	Activates all station account event debug messages.
<extension>	Optional. Activates station account event debug messages for a specific extension.
summary	Activates simple voice event debug messages.
switchboard	Activates all switchboard event debug messages.
<subsource>	Optional. Activates switchboard event debug messages for a specific subsource.
call	Activates switchboard call state machine event debug messages.
call *<call id>*	Optional. Activates switchboard call state machine event debug messages for a specific call.
ccm	Activates switchboard call connection manager event debug messages.
toneservices	Activates all tone service events debug messages.
<notifies>	Optional. Activates tone service events debug messages for the specified interface type. For example, for a foreign exchange station (FXS) interface, use **fxs**.
<interface>	Optional. Activates tone service events debug messages for the specified interface type.
<interface> <slot/port>	Optional. Activates tone service events debug messages for the specified slot and port of the interface type. For example, for an individual FXS port use, **fxs 0/1**.
trunkaccount	Activates all trunk account event debug messages.
<trunk id>	Optional. Activates trunk account event debug messages for a specific trunk.

<trunk id> <appearance>	Optional. Specifies specific trunk appearance.
trunkmanager	Activates all trunk manager event debug messages.
<trunk id>	Optional. Activates trunk manager event debug messages for a specific trunk.
<trunk id> <appearance>	Optional. Specifies specific trunk appearance.
trunkport	Activates all trunk port event debug messages.
<slot:port:DS0>	Optional. Activates trunk port event debug messages for a specific slot, port, and digital signal 0 (DS0).
verbose	Optional. Displays the entire running configuration to the terminal screen (versus only the nondefault values).

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 9.3	Command was introduced.
Release 10.1	Command was expanded to include more parameters.
Release 12.1	Command was expanded to include more parameters.
Release 13.1	Command was expanded to include more parameters.
Release 14.1	Command was expanded to include more parameters.
Release 15.1	Command was expanded to include more parameters.
Release A1	Command was expanded to include the **loopback** parameter.
Release A2	Command was expanded to include the **conference local** and **dsp** parameters.
Release A2.04	Command was expanded to include the **erltool**, **paging-group**, and **replication** parameters.
Release A4.01	Command was expanded to include the **moh**, **findme-followme**, **pickup-group**, **queue**, and **conference local** parameters.
Release A4.05	Command was altered to exclude the **color** and **pickup-group** parameters. The **color** parameter is covered by the **debug color** command on *page 298* and the **pickup-group** parameter is covered using the **debug voice verbose** command. Command was expanded to include the **services-interface** and **ring-group** parameters.
Release A5.01	Command was expanded to include the **fax**, **detailed**, and **isu_cp_det** parameters.
Release R11.2.0	Command was expanded to include the **call-pickup** parameter.
Release R11.5.0	Command was expanded to include the **srtp** and **sdes** parameters.

Release R13.6.0	Command was rewritten to exclude parameters that are no longer supported (**auto-attendant**, **call-pickup**, **dsp fax**, **dsp isu_cp_det**, **findme-followme**, **mail**, **moh**, **paging-group**, **promptstudio**, **proxydial**, **queue**, **replication**, **services interface**, and **statusgroups**). In addition the **rtp** parameter was added to the **debug voice dsp voip** command, the **rtp** and **rfc2833** parameters were added to the **debug dsp voip verbose** command, the <*group*> parameter was added to the **debug voice ring-group** command, the <*appearance*> parameter was added to the **debug voice trunkmanager** command.

Usage Examples

The following example activates all debug messages associated with voice functionality:

>**enable**
#debug voice summary

debug vrrp

Use the **debug vrrp** command to enable Virtual Router Redundancy Protocol (VRRP) debug messages. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug vrrp
debug vrrp error
debug vrrp interface <*interface*> **error**
debug vrrp interface <*interface*> **group** <*number*> **error**
debug vrrp interface <*interface*> **group** <*number*> **packet**
debug vrrp interface <*interface*> **packet**
debug vrrp packet

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

error	Optional. Displays debug messages for all VRRP errors in all groups on all interfaces or on a specified interface.
interface <*interface*>	Optional. Displays debug messages for all VRRP groups on the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network (VLAN) interface, use **vlan 1**. Type **debug vrrp interface ?** for a complete list of valid interfaces.
group <*number*>	Optional. Specifies debug messages for a single VRRP group on a specified interface are generated. Group numbers range from **1** to **255**.
error	Optional. Displays debug messages for VRRP errors for a single group on a specified interface.
packet	Optional. Displays debug messages for VRRP packets for a single group on a specified interface.
packet	Optional. Displays debug messages for all VRRP packets in all groups on all interfaces or on a specified interface.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release 16.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

Although VRRP group virtual router IDs (VRIDs) can be numbered between 1 and 255, only two VRRP routers per interface are supported.

Usage Examples

The following example gives sample output from the **debug vrrp packet** command:

>**enable**
#debug vrrp packet
2007.05.26 15:48:57 VRRP.PKT eth 0/1 grp 1 Sent Advertisement pri: 125, ipCnt:1
2007.05.26 15:48:57 VRRP.PKT eth 0/1 grp 2 Received Advertisement pri: 125 from 10.23.197.236

debug vrrpv3

Use the **debug vrrpv3** command to enable Virtual Router Redundancy Protocol version 3 (VRRPv3) debug messages. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages. Variations of this command include the following:

debug vrrpv3
debug vrrpv3 error
debug vrrpv3 interface <*interface*>
debug vrrpv3 interface <*interface*> **group** <*vrid*> **ipv4**
debug vrrpv3 interface <*interface*> **group** <*vrid*> **ipv6**
debug vrrpv3 interface <*interface*> **group** <*vrid*> **ipv4 packet**
debug vrrpv3 interface <*interface*> **group** <*vrid*> **ipv6 packet**
debug vrrpv3 interface <*interface*> **packet**
debug vrrpv3 packet

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

error	Optional. Displays debug messages for all VRRPv3 errors in all groups on all interfaces or on a specified interface.
interface <*interface*>	Optional. Displays debug messages for all VRRPv3 groups on the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network (VLAN) interface, use **vlan 1**. Type **debug vrrpv3 interface ?** for a complete list of valid interfaces.
group <*vrid*>	Optional. Displays debug messages for a single VRRPv3 virtual router ID (VRID) on a specified interface. VRIDs range from **1** to **255**.
ipv4	Displays debug messages for the VRID's IPv4 address family.
ipv6	Displays debug messages for the VRID's IPv6 address family.
packet	Optional. Displays debug messages for VRRPv3 packets for a single group on a specified interface.
packet	Optional. Displays debug messages for all VRRPv3 packets in all groups on all interfaces or on a specified interface.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R10.7.0	Command was introduced.
Release R10.11.0	Command was expanded to include the **ipv4** and **ipv6** parameters.

Functional Notes

Although VRRPv3 group VRIDs can be numbered between 1 and 255, only two VRRPv3 routers per interface per IP version are supported.

Usage Examples

The following example enables VRRPv3 debug messaging:

>**enable**
#debug vrrpv3 packet

debug y1731 file-save

Use the **debug y1731 file-save** command to enable debug messages for the Y.1731 performance monitoring logging subsystem to display information on file writes and log rotation events. Use the **no** form of this command to disable the debug messages.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in AOS are disabled.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example enables Y.1731 performance monitoring logging debug messaging:

```
>enable
#debug y1731 file-save
```

dir

Use the **dir** command to display a directory list of all files on the system or just those matching the specified pattern, located in a specified location. Variations of this command include:

dir
dir *<pattern>*
dir cflash
dir cflash *<pattern>*
dir flash
dir flash *<pattern>*
dir ramdisk
dir ramdisk *<pattern>*
dir usbdrive0
dir usbdrive0 *<pattern>*

Syntax Description

<pattern>	Optional. Displays all files that match the specified pattern. When a wildcard (*****) is specified, only files located in the specified location matching the listed pattern are displayed. For example, ***.biz** displays all files with the .biz extension. When no wildcard is specified, the entire contents of flash memory is displayed.
cflash	Optional. Displays files located on the installed CompactFlash® card.
flash	Optional. Displays files located on the system in flash memory.
ramdisk	Optional. Displays files located on the volatile RAM disk.
usbdrive0	Optional. Displays files located on the Universal Serial Bus (USB) flash drive memory.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 12.1	Command was expanded to include CompactFlash.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include USB flash drive memory.

Usage Examples

The following is sample output from the **dir flash** command:

```
>enable
#dir flash
3563529 NV2100A-10-05-00-E.biz
   2438 startup-config
   2484 startup-config.bak
3694712 bytes used, 3007368 available, 6702080 total
```

The following is sample output from the **dir ramdisk** command displaying the contents of the RAM disk, space occupied by each file, the total ramdisk space allocated, available space, and used space:

```
>enable
#dir ramdisk
10005125 NV3130A-17-07-00-26-AE.biz
10007923 bytes used, 7429514 available, 17437437 total
```

disable

Use the **disable** command to exit the Enable mode and enter the Basic mode.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example exits the Enable mode and enters the Basic Command mode:

```
#disable
>
```

dot11ap apply-changes

Use the **dot11ap apply-changes** command to apply any configuration changes to a NetVanta 160 Series access point (AP). Any configuration that is performed on the AP is not completed until the configuration is applied to the AP using this command. Variations of this command include:

dot11ap apply-changes <*ap*>
dot11ap apply-changes all

Syntax Description

<*ap*>	Specifies the NetVanta 160 Series AP to which to apply the changes. Valid range is **1** to **8**.
all	Optional. Specifies the changes are applied to all managed NetVanta 160 Series APs.

Default Values

By default, no changes are applied to the NetVanta 160 AP without the use of this command.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example specifies that all NetVanta 160 Series APs managed by the access controller are updated with recent configuration changes:

>**enable**
#dot11ap apply-changes

eject usbdrive0

Use the **eject usbdrive0** command to safely eject a specified Universal Serial Bus (USB) device before removing it from the AOS unit.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example ejects an attached USB flash drive device.

```
>enable
#eject usbdrive0
```

erase

Use the **erase** command to erase the files from a specified location.

Variations of this command (valid on all AOS units) include:

erase *<filename>*
erase startup-config

Variations of this command (valid only on AOS units WITH CompactFlash®) include:

erase cflash *<filename>*
erase flash *<filename>*
erase file-system cflash

Variations of this command (valid only on AOS units WITH voice capability) include:

erase dynvoice-config
erase file-system flash
erase file-system interface mef-ethernet *<interface>*

Variations of this command (valid only on AOS units WITH **ramdisk** enabled) include:

erase ramdisk *<filename>*

Variations of this command (valid only on AOS units WITH Universal Serial Bus (USB) flash drive capability) include:

erase file-system usbdrive0
erase usbdrive0 *<filename>*

Erasing the file system removes all files and directories located in the unit's memory, including firmware images. If the primary boot image is located on the erased file system, the unit will be adversely affected after a reboot. The firmware has to be replaced using the procedure explained in the Upgrading AOS Firmware configuration guide, available online at https://supportcommunity.adtran.com.

Syntax Description

<filename>	Specifies the name of the file to erase. The asterisk (*) can be used as a wildcard to specify a pattern for erasing multiple files. When a wildcard is specified, only files matching the listed pattern are erased.
cflash	Specifies the location of the file to erase as the installed CompactFlash card.
dynvoice-config	Erases the dynamic voice configuration file stored in the flash memory.
file-system	Erases the system files stored in either the system flash, CompactFlash, or USB flash drive memory.
flash	Specifies the location of the file to erase as the system flash memory.
mef-ethernet *<interface>*	Erases the file system on the specified MEF-Ethernet interface.

ramdisk	Specifies the location of the file to erase as the volatile RAM disk.
startup-config	Erases the startup configuration file stored in flash memory.
usbdrive0	Specifies the location of the file to erase as the USB flash drive memory.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 12.1	Command was expanded to include the **dynvoice-config** parameter.
Release 14.1	Command was expanded to include the **file-system cflash** parameter.
Release A2.04	Command was expanded to include the **file-system flash** parameter.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release 18.2	Command was expanded to include the USB flash drive memory.

Usage Examples

The following example erases the startup configuration file stored in flash memory:

>**enable**
#erase startup-config
If a new startup configuration file is not specified before cycling the power on the unit, AOS will initialize using a blank configuration.

The following example erases all files located on the installed CompactFlash card:

>**enable**
#erase file-system cflash
This will erase ALL files on compact flash. Proceed? [y/n]

The following example erases all files located in the system flash memory:

>**enable**
#erase file-system flash
WARNING! You are about to erase all files on the flash file system.
This includes all firmware images and configuration files. This cannot be undone.

This will erase ALL files on flash. Proceed? [y/n]

events

Use the **events** command to enable event reporting to the current command line interface (CLI) session. Use the **no** form of this command to disable all event reporting to the current CLI session.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example enables event reporting:

```
>enable
#events
```

exception report generate

Use the **exception report generate** command to immediately generate an exception report.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example immediately generates an exception report:

```
>enable
#exception report generate
```

factory-default

Use the **factory-default** command to reset the unit to the factory default setting.

*Performing an AOS **factory-default** disrupts data traffic.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

After you issue this command, the system responds by first warning you that restoring the factory default settings will erase the current configurations. It then asks if you would like to proceed. Choose **n** to return to the command prompt (no configuration changes are made). Choose **y** to erase the startup-configuration, replace it with the factory-default configuration, and reboot the unit. After reboot, the new configuration takes effect.

Usage Examples

The following example resets the unit to the factory default settings:

>**enable**
#factory-default

WARNING - Restoring the factory default settings will erase the current startup and running configurations and will reboot the unit.

Restore factory default settings?[y/n]**y**

Startup configuration written.

Rebooting the system. Please wait...

find <*input*>

Use the **find** command to search the AOS CLI for a specific command. The output of this command displays the command set location of the discovered commands. Variations of this command include:

find <*input*>
find /current set <*input*>
find /current set /no suppress <*input*>
find /no suppress /current set <*input*>
find /no suppress <*input*>

Syntax Description

<*input*>	Specifies the given command for which to search in a text string; for example, **sip proxy**. Wild-card matching can be performed by entering *****; for example, **sip ***.
/current set	Optional. Limits the command search results to the current command set.
/no suppress	Optional. Specifies the search output does not suppress multiple results.

Default Values

No default values are necessary for this command.

Command History

Release R12.1.0	Command was introduced.

Functional Notes

The **/current set** and **/no suppress** parameters of the **find** command may be entered in any order.

The use of wildcard matching can be beneficial when searching for a command for which the entire command syntax is not known (such as **sip pr**).

Usage Examples

The following example searches for the command **billing-code**:

```
>enable
#find billing-code
Searching.... Found 2 commands
voice-user          : billing-codes
configterminal      : voice spre-map billing-code
```

The following example searches for any commands with **sip pr**:

```
>enable
#find sip pr
Searching...Found 4 commands
Root                : clear sip proxy
```



```
Root                : debug sip proxy
Root (2)            : show sip proxy
configterminal      : sip proxy
```

The following example searches for any commands with **sip pr**, without suppressing the search results:

```
>enable
#find /no-suppress sip pr
Searching... Found 7 commands
Root                : clear sip proxy
Root                : debug sip proxy
Root                : show running-config sip proxy
Root                : show sip proxy
configterminal      : sip prefer
configterminal      : sip privacy
configterminal      : sip proxy
```


flashme

Use the **flashme** command to allow the ActivChassis master device to flash the LEDs on its connected linecard devices. Variations of this command include:

flashme
flashme vcid <*vcid*>
flashme vcid <*vcid*> <*value*>
flashme <*value*>

Syntax Description

vcid <*vcid*>	Optional. Specifies that only the device with the specified VCID will flash LEDs. Valid VCID range is **1** to **8** (VCID values **1** and **2** are given to the ActivChassis master and backup devices, respectively).
<*value*>	Optional. Specifies the duration (in seconds) that the LEDs will flash.

Default Values

By default, LEDs will flash for **3** seconds.

Command History

Release AC1.0	Command was introduced.

Functional Notes

This command is available from both the ActivChassis master and linecard devices' CLI. For more information about the difference between linecard and master devices, how to access the CLI for each, and additional configuration information, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example tests the master device's connection to all ActivChassis linecard devices:

>enable
#flashme

http secure-server certificate regenerate

Use the **http secure-server certificate regenerate** command to generate a new private key and certificate used by the Hypertext Transfer Protocol (HTTP) secure (HTTPS) server. When a new HTTPS certificate is generated, it erases the old HTTPS private key and certificate.

Syntax Description

No subcommands.

Default Values

By default, a unique HTTPS certificate and private key are generated when the system boots for the first time.

Command History

Release R11.7.0	Command was introduced.

Usage Examples

The following example generates a new https certificate:

```
(config)#http secure-server certificate regenerate
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         70:a2:aa:7c:8e:d8:ef:b2:68:e1:58:65:55:84:69:81:19:91:7b:29
   Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=US, ST=AL, L=Huntsville, O=Adtran, Inc., CN=NetVanta
      Validity
         Not Before: Jun 19 19:11:09 2015 GMT
         Not After : Jun 17 19:11:09 2023 GMT

-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIUcKKqfI7Y3bJo4VhlVYRpgRmReykwDQYJKoZIhvcNAQEL
BQAwWTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkFMMRMwEQYDVQQHDApIdW50c3Zp
dHN2aWxsZTELMAkGA1UEBhMCVVMwHhcNMTUwNDI5MDY0ODE0WhcNMjMwNDI3MDY0
DTE1MDYxOTE5MTEwOVoXDTIzMDYxNzE5MTEwOVowWTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgMAkFMMRMwEQYDVQQHDApIdW50c3ZpbGxlMRUwEwYDVQQKDAxBRFRSQU4s
IEluY4xETAPBgNVBAMMCE5ldFZhbnRhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2x/r4499jQKrXX0810fTkIoGk5jNwkfQ7JkZxSoqX7OPzYSYQ8/E
1UF/fsv0SxlHCTVTVmihLSbkc75fDEs6NL3URGFXBLJJ/Rlg5g3UwdnpUR02GUr3
zP7kXP+UvcuUWD7DqamcD2eS/78sn6kZUVE+ocytr89KDsevU/eRhEvUq2Z3YgIA
3fg3hGYYD2vTSarWOmRd3cFxzw7C2TTUnHCVu+CCVxvOmETFljfHwjOl1KgBBTVe
o2rR+Yyb5RtUiPmyQdVeR8L6OBV0/yToF4/AX73gUiOjMOeiPZ30SQPIJhjumVvV
FC1w8CfHALoDjbpBGqwIuxO9XjqtIdxe7QIDAQABoy8wLTAMBgNVHRMBAf8EAjAA
MB0GA1UdDgQWBBTyhd5mKbpAOtV03ObopcGtuYFg8TANBgkqhkiG9w0BAQsFAAOC
```

AQEAk3E3ea3esaLf4KgbXvViBIT0/S9+P6gmU88hZcyr6/ArOzpSv0Ne21orByk3
OsBBFoGibMfOYzRL8tPD3b5aqqwjDlXmG2rg8i1W/tLDeyo6xDPrxJEN+3EEqLIP
3EKEVAyL1a6DaeQOvv3B5tN28mmLYCxP5749gcnE3jIH77cCxLrxR1HcvGlelecw
yi8RioKBho/yOl5jCR4VTgDYzXhbrdSheuVAsjoEb1yaNi00sKlJbfIneHlUfYK9
gD0rBw5hoW7QxSx7N/oo3D/7yKxN5aKyCAJwlfyRWeytSrVc9UgoXzD4PNu7UiYz
jtgSsHe4c5Vwx8xS+0G9ttf42w==
-----END CERTIFICATE-----

ip dhcp

Use the **ip dhcp** command to manually release or renew Dynamic Host Control Protocol (DHCP) values. Releasing DHCP values causes the DHCP client to stop using information assigned by the DHCP server and releases that information. Renewing DHCP values causes the DHCP client to re-request information. Variations of this command include:

ip dhcp release
ip dhcp release <*interface*>
ip dhcp release efm-group <*group id*>
ip dhcp release mef-ethernet <*slot/port*>
ip dhcp release system-control-evc
ip dhcp release system-management-evc
ip dhcp renew
ip dhcp renew <*interface*>
ip dhcp renew efm-group <*group id*>
ip dhcp renew mef-ethernet <*slot/port*>
ip dhcp renew system-control-evc
ip dhcp renew system-management-evc

Syntax Description

<*interface*>	Optional. Specifies that DHCP information is released or renewed on the single interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **ip dhcp release ?** at the prompt.
efm-group <*group id*>	Specifies an Ethernet in the first mile (EFM) group ID. Range is **1** to **1024**.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies that DHCP information is released or renewed on the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Specifies that DHCP information is released or renewed on the system management EVC.

Default Values

By default, if DHCP has been enabled, then the IA_NA is released or renewed. If DHCP has not been enabled, then only non-address configuration information is released or renewed.

Command History

Release R11.1.0	Command was introduced.
Release R11.3.0	Command was expanded to include the Ethernet in the first mile (EFM) group and Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example manually renews all non-address DHCP information:

>**enable**
#ip dhcp renew

ipv6 dhcp

Use the **ipv6 dhcp** command to release or renew Dynamic Host Control Protocol version 6 (DHCPv6) values manually. Releasing DHCPv6 values causes the DHCPv6 client to stop using information assigned by the DHCPv6 server and releases that information. Renewing DHCPv6 values causes the DHCPv6 client to rerequest information. Variations of this command include:

ipv6 dhcp release
ipv6 dhcp release address
ipv6 dhcp release address <*interface*>
ipv6 dhcp release all
ipv6 dhcp release all <*interface*>
ipv6 dhcp release information
ipv6 dhcp release information <*interface*>
ipv6 dhcp release prefix
ipv6 dhcp release prefix <*interface*>
ipv6 dhcp renew
ipv6 dhcp renew address
ipv6 dhcp renew address <*interface*>
ipv6 dhcp renew all
ipv6 dhcp renew all <*interface*>
ipv6 dhcp renew information
ipv6 dhcp renew information <*interface*>
ipv6 dhcp renew prefix
ipv6 dhcp renew prefix <*interface*>

Syntax Description

address	Optional. Specifies that only the DHCPv6 identity association non-temporary address (IA_NA) is released or renewed.
all	Optional. Specifies that all DHCPv6 values are released or renewed.
information	Optional. Specifies that only DHCPv6 non-address configuration information is released or renewed.
prefix	Optional. Specifies that only the DHCPv6 identity association prefix definition (IA_PD) is released or renewed.
<*interface*>	Optional. Specifies that DHCPv6 information is released or renewed on the single interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **ipv6 dhcp release ?** at the prompt.

Default Values

By default, if DHCPv6 has been enabled, then the IA_NA is released or renewed. If DHCPv6 has not been enabled, then only non-address configuration information is released or renewed.

Command History

Release R10.9.0	Command was introduced.
Release R10.11.0	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example manually renews non-address DHCPv6 information:

>**enable**
#ipv6 dhcp renew information

led status-led

Use the **led status-led** command to control the status LED on an applicable AOS device. This command can be used to turn off the LED, as well as control both the LED color and blink rate. Use the **no** form of this command to return to the default setting. Variations of this command include:

led status-led [green | red]
led status-led [green | red] blink [fast | slow]
led status-led red-green
led status-led off

Syntax Description

green	Modifies the status LED display to green.
red	Modifies the status LED display to red.
red-green	Modifies the status LED to alternate between red and green
blink	Specifies the status LED blink rate. If the blink rate is not specified, the display color will be solid (i.e., non-blinking).
fast	Specifies a blink rate of five times per second.
slow	Specifies a blink rate of once per second.
off	Turns off the status LED.

Default Values

By default, the status LED is solid green.

Command History

Release R11.6.0	Command was introduced.
Release R11.7.0	Command was expanded to include the **red-green** parameter.

Functional Notes

This command does not save to the startup configuration file. When the device reboots, the status LED display returns to the default setting.

Usage Examples

The following example changes the status LED display to slow, blinking red:

>enable
#led status-led red blink slow

license activate <*activation key*>

Use the **license activate** <*activation key*> command to specify up to five license activation keys for activating licensed features on your AOS device.

Syntax Description

<*activation key*>	Specifies the activation key to use for licensing AOS features. Up to **5** activation keys can be entered using this command.

Default Values

No default values are necessary for this command.

Command History

Release R13.4.0	Command was introduced.

Functional Notes

The activation keys used in this command are provided to you by Adtran when you purchase AOS features. When this command is issued, the entered activation keys are automatically sent to a licensing server (specified using the command *license server on page 1570*), and then the features are automatically licensed on the AOS unit.

This two-step licensing procedure, configuring a license server and activating license keys, replaces the four-step licensing process introduced in AOS firmware release R11.8.0. For more information about the AOS feature licensing process, refer to the quick start guide, *Licensing AOS Features*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example three activation keys are sent to the licensing server for automatic feature licensing on the AOS device:

```
>enable
#license activate key1 key2 key3 key 4 key 5
```


license capability

Options for licensing AOS features depends on the AOS firmware installed on the AOS device. The AOS firmware 14.3.0 supports both Legacy Licensing and New Licensing solutions. The New Licensing solution is streamlined into a 4-step process which is configurable using AOS CLI or GUI.

license capability request
license capability request key <actId1>
license capability request key <actId1> <actId2>
license capability request key <actId1> <actId2> <actId3>
license capability request key <actId1> <actId2> <actId3> <actId4>
license capability request key <actId1> <actId2> <actId3> <actId4> <actId5>
license capability response key install *<filename>*
license capability response key uninstall

Syntax Description

request	Manage the capability request
key	Generate the capability request bin file without specifying the activation IDs.
<**Activation Id**>	Optional. Specify the activation IDs up to a maximum of 5 Activation IDs for generating the capability request bin file.
response	Install or uninstall a software license from the unit.
key	Install or uninstall a software license from the unit.
install	Install a software license.
file	Specifies the software license file.
<filename>	Specifies the capability response bin file to install the license.
uninstall	Uninstalls the software license.

Default Values

No default values are necessary for this command.

Command History

Release R14.3.0	Command was introduced.

Functional Notes

AOS uses two types of key files for activating licensed AOS features.

Activate by using the capability response file:

The capability response file is obtained from the Adtran licensing portal for the AOS features purchased on your adtran email account. The capability response file can be imported to the device's flash and installed using the CLI “license capability response key install file <filename>” to activate the purchased AOS features.

Activate by using the Capability request file:

Before you begin, you must verify that you have your Activation key(s) for each AOS feature you want to license in the confirmation email after your purchase. Next, you will generate a License Capability Request bin file from the AOS unit on which you want to enable the newly purchased features. The generated License Capability Request bin file is saved to the device's flash. The bin file is then exported through secure copy or tftp to your machine. This will generate the capability Response bin file from Adtran licensing portal.The capability response downloaded will have the license mapped to your device with your existing call capacity and features. The capability response is imported to the Device Flash and installed using “license capability response key install file <filename>” command which activates the AOS features.

Usage Examples

Providing activation IDs is optional. The following example generates a capability request without any activation IDs. The capability request file is then exported to the Adtran licensing server to generate and download the capability response file for installing the license on your device.

>**enable**
#license capability request key

The following example generates the capability request that sets activation IDs that you received when you registered your Adtran email account.

>**enable**
#license capability request key actId1 actId2 actId3

The following example installs the capability response bin file <capabilityResponse.bin> on the unit for activating AOS features.

>**enable**
#license capability response key install file capabilityResponse.bin
The following example uninstalls the software license from device. A reboot is required on the unit after the uninstall command is issued to ensure the software license was completely removed.

>**enable**
#license capability response key uninstall
#reload

license key

Use the **license key** command to install or remove license keys for the purpose of enabling AOS features on a device. Variations of this command include:

license key install
license key install file *<filename>*
license key uninstall all
license key uninstall invalid
license key uninstall unsupported
license key uninstall *<software license serial number>*

Syntax Description

install	Indicates that a license key is about to be entered into the AOS device. Once entered, this command prompts the user for input (as shown in the **Usage Examples** below) unless the command includes the **file** *<filename>* parameter.
file *<filename>*	Optional. Specifies a file name for installing a license key.
uninstall	Specifies removing license keys on the system.
all	Specifies removing all license keys.
invalid	Specifies removing invalid license keys only.
unsupported	Specifies removing unsupported license keys only.
<serial number>	Specifies a license serial number to remove.

Default Values

No default values are necessary for this command.

Command History

Release R11.8.0	Command was introduced.

Functional Notes

AOS uses two types of keys for enabling additional licensed AOS features. The license key is obtained from the Adtran licensing portal and installed on the AOS device in order to activate additional features. This process of obtaining a license key requires a second key, called a license request key (or a challenge key). The license request key is a unique key generated by AOS and contains information about the unit that validates it for a one time use only. Once a license key has been installed, the license request key is cleared and no longer valid.

The **license request key** command will not display a key until the **license request key generate** command has been issued for the first time. Generating a new license request key clears any previous license request keys, in which case a warning is issued.

Usage Examples

The following example prepares AOS to receive a license key to enable additional features:

>**enable**
#license key install
Enter the entire license key. End with two consecutive
carriage returns or the word "quit" on a line by itself:
quit

The following example removes all license keys currently on the device:

>**enable**
#license key uninstall all

license request key

Use the **license request key** command to view or generate a license request (challenge) key which is used to request a license key for enabling AOS features on a device. Variations of this command include:

license request key
license request key generate

Syntax Description

generate	Optional. Generates a license request key.

Default Values

No default values are necessary for this command.

Command History

Release R11.8.0	Command was introduced.

Functional Notes

AOS uses two types of keys for enabling additional licensed AOS features. The license key is obtained from the Adtran licensing portal and installed on the AOS device in order to activate additional features. This process of obtaining a license key requires a second key, called a license request key (or a challenge key). The license request key is a unique key generated by AOS and contains information about the unit that validates it for a one time use only. Once a license key has been installed, the license request key is cleared and no longer valid.

The **license request key** command will not display a key until the **license request key generate** command has been issued for the first time. Generating a new license request key clears any previous license request keys, in which case a warning is issued.

Usage Examples

The following example generates a license request key:

```
>enable
#license request key generate

WARNING!
This will generate a new license request key.
You will not be able to install licenses that
were requested using any previous license request key.

This action is irreversible.

Proceed? [yes/no]
```


The following example displays the current active license request key:

>**enable**
#license request key

license unit identifier

Use the **license unit identifier** command to view the unit identification (ID) used for requesting AOS feature license keys.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.8.0	Command was introduced.

Functional Notes

The unit ID is a unique number that identifies a specific AOS unit. It is included in the license request key sent to the Adtran licensing portal.

AOS uses two types of keys for enabling additional licensed AOS features. The license key is obtained from the Adtran licensing portal and installed on the AOS device in order to activate additional features. This process of obtaining a license key requires a second key, called a license request key (or a challenge key). The license request key is a unique key generated by AOS and contains information about the unit that validates it for a one time use only. Once a license key has been installed, the license request key is cleared and no longer valid.

The **license request key** command will not display a key until the **license request key generate** command has been issued for the first time. Generating a new license request key clears any previous license request keys, in which case a warning is issued.

Usage Examples

The following example displays the current unit identifier:

```
>enable
#license unit identifier
```

logout

Use the **logout** command to terminate the current session and return to the login screen.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the logout command being executed in Enable mode:

```
>enable
#logout
Session now available
Press RETURN to get started.
```


mount usbdrive0

Use the **mount usbdrive0** command to mount a Universal Serial Bus (USB) flash drive device.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example mounts a USB flash drive device onto the AOS unit:

```
>enable
#mount usbdrive0
```

nslookup

Use the **nslookup** command to view and troubleshoot domain naming system (DNS) information by querying the configured or specified DNS server. Variations of this command include:

nslookup
nslookup <*hostname* | *ip address*>
nslookup <*hostname* | *ip address*> **server** <*hostname* | *ip address*>
nslookup <*hostname* | *ip address*> **server** <*hostname* | *ip address*> **type** <*type*>
nslookup <*hostname* | *ip address*> **type** <*type*>
nslookup vrf <*name*>
nslookup vrf <*name*> <*hostname* | *ip address*>
nslookup vrf <*name*> <*hostname* | *ip address*> **server** <*hostname* | *ip address*>
nslookup vrf <*name*> <*hostname* | *ip address*> **server** <*hostname* | *ip address*> **type** <*type*>
nslookup vrf <*name*> <*hostname* | *ip address*> **type** <*type*>

Syntax Description

<*hostname* | *ip address*>	Specifies the fully qualified domain name (FQDN) or destination IP address to be used as the target of the DNS query. IPv4 addresses should be expressed in dotted decimal notation (for example, **208.61.209.1**). IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).
server <*hostname* | *ip address*>	Optional. Specifies the FQDN or IP address of the DNS server to query.
type <*type*>	Optional. Specifies the type of DNS query. Supported query types include: **A**, **AAAA**, **SRV**, **SOA**, **CNAME**, **PTR**.
vrf <*name*>	Optional. Specifies the non-default virtual routing and forwarding (VRF) instance on which the DNS query will be sent.

Default Values

No default values are necessary for this command.

Command History

R13.3.0	Command was introduced.

Usage Examples

The following example returns the result of a DNS **A** record query for **www.example.com** from the server at **198.51.100.1**:

>**enable**
#nslookup www.example.com server 198.51.100.1 type a
DNS Server: 198.51.100.1 53

ANSWER SECTION:
Host : www.example.com
Type : A
TTL : 6662
Address : 198.51.100.100

ping

Use the **ping** command (at the Enable mode prompt) to verify IPv4 network connectivity. For information on how to verify IPv6 network connectivity, refer to *ping ipv6 on page 520*. Variations of this command include:

ping
ping [ip] <*ipv4 address* | *hostname*>
ping [ip] <*ipv4 address* | *hostname*> <*interface*>
ping [ip] <*ipv4 address* | *hostname*> **data** <*string*>
ping [ip] <*ipv4 address* | *hostname*> **df-bit [0 |1]**
ping [ip] <*ipv4 address* | *hostname*> **dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]**
ping [ip] <*ipv4 address* | *hostname*> **repeat** <*number*>
ping [ip] <*ipv4 address* | *hostname*> **size** <*value*>
ping [ip] <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
ping [ip] <*ipv4 address* | *hostname*> **mef-ethernet** <*slot/port*>
ping [ip] <*ipv4 address* | *hostname*> **system-control-evc**
ping [ip] <*ipv4 address* | *hostname*> **system-management-evc**
ping [ip] <*ipv4 address* | *hostname*> **timeout** <*value*>
ping [ip] <*ipv4 address* | *hostname*> **tos** <*value*>
ping [ip] <*ipv4 address* | *hostname*> **verbose**
ping [ip] <*ipv4 address* | *hostname*> **wait** <*interval*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> <*interface*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **data** <*string*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **df-bit [0 |1]**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **repeat** <*number*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **size** <*value*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **mef-ethernet** <*slot/port*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **system-control-evc**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **system-management-evc**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **timeout** <*value*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **tos** <*value*>
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **verbose**
ping [ip] vrf <*name*> <*ipv4 address* | *hostname*> **wait** <*interval*>

After specifying the target IPv4 address to ping, the other parameters can be entered in any order. Use the ***?*** *after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

ip	Optional. Specifies an IPv4 ping.
<*interface*>	Optional. Specifies the egress interface when pinging an IPv4 address. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **ping** <*ipv4 address* | *hostname*> **?** to display a list of valid interfaces.
<*ipv4 address* | *hostname*>	Optional. Specifies the IPv4 address or host name of the system to ping. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Entering the **ping** command with no specified Internet Protocol version 4 (IPv4) address prompts the user with parameters for a more detailed **ping** configuration. Refer to *Functional Notes* (below) for more information.
data <*string*>	Optional. Specifies an alphanumerical string to use (the ASCII equivalent) as the data pattern in the ECHO_REQ packets.
df-bit 0	Optional. Specifies that the Don't Fragment (DF) bit in the IP header is not set.
df-bit 1	Optional. Specifies setting the DF bit in the IP header. This will prevent the ping packets from being fragmented along the way.
dscp	Optional. Specifies the differentiated services code point (DSCP) value.
<*value*>	Optional. Valid range is decimal **0** to **63**. The value can also be specified in hexadecimal by adding a **0x** prefix to the number.
af*xx*	Optional. Specifies the assured forwarding (AF) class and subclass for the DSCP value. Select from: 11 (001010), 12 (001100), 13 (001110), 21 (010010), 22 (010100), 23 010110), 31 (011010), 32 (011100), 33 (011110), 41 (100010), 42 (100100), or 43 (100110).
cs*x*	Optional. Specifies the class selector (CS) value for the DSCP value. Valid range for *x* is **0** to **7**.
default	Optional. Specifies default (000000) DSCP value.
ef	Optional. Specifies expedited forwarding (EF) (101110) for the DSCP value.
repeat <*number*>	Optional. Specifies the number of loopback messages to be sent. Range is **1** to **1024**.
size <*value*>	Optional. Specifies the datagram size (in bytes) of the ping packet. Valid range is **1** to **65507** bytes. Except for most switches which have a maximum of **29000**.
source <*ipv4 address*>	Optional. Specifies the IPv4 address to use as the source address in the ECHO_REQ (or interface) packets. The source IPv4 address must be a valid address local to the router on the specified virtual routing and forwarding (VRF) instance.
mef-ethernet <*slot/port*>	Optional. Specifies the Metro Ethernet Forum (MEF) Ethernet interface as the ping target.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC) as the ping target.
system-management-evc	Optional. Specifies the system management EVC as the ping target.

tos <*value*>	Optional. Specifies the type of service (ToS). The <*value*> can be specified as decimal (**0** to **255)** or as hexidecimal.
timeout <*value*>	Optional. Specifies the timeout period after which the ping is considered unsuccessful. Valid range is **1** to **60** seconds.
verbose	Optional. Enables detailed messaging.
vrf <*name*>	Optional. Specifies the VRF where the IPv4 address exists.
wait <*interval*>	Optional. Specifies a minimum time to wait between sending test packets. Valid range is **100** to **60000** milliseconds.

Default Values

By default, the **data** pattern is set to **abcd**.

By default, the **df-bit** is set to **0**.

By default, the **repeat** is set to **5**.

By default, the **size** value is set to **100** bytes.

By default, the **timeout** value is set to **2** seconds.

By default, the **wait** value is set to **100** milliseconds.

Command History

Release 1.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 17.2	Command was expanded to include the **verbose** and **wait** parameters, also changes were made to the **repeat** and **timeout** values.
Release 17.4	Command was expanded to include the **count** and **interval** parameters. The **repeat** and **wait** parameters were removed.
Release A4.01	Command was expanded to return the **wait** parameter.
Release 18.3.0	Command was expanded to include the optional **ip** and <*interface*> parameters.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the **df-bit**, **dscp**, **system-control-evc**, **system-management-evc**, and **tos** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R11.1.0	Functional Notes were enhanced to explain parameter behaviour with multiple entries.

Functional Notes

The **ping** command can be issued from both the Basic and Enable modes.

The **ping** command helps diagnose basic IPv4 network connectivity using the Packet Internet Groper program to repeatedly bounce Internet Control Message Protocol version 4 (ICMPv4) ECHO_REQ packets off a system (using a specified IPv4 address). AOS allows executing a standard **ping** request to a specified IP address, or provides a set of prompts to configure a more specific **ping** configuration.

After specifying the target IPv4 address (or hostname) to ping, the following parameters can be entered multiple times and in any order: **data**, **df-bit**, **repeat**, **size**, **source**, and **timeout**. When entering multiple instances of the same parameter, the last entry will be used. In the following example syntax, only the last entries for **data**, **repeat**, and **size** will be used, ignoring previous entries for these parameters:

ping ip 192.0.2.15 size 600 data bbbb repeat 3 size 300 data aaaa repeat 2 verbose dscp cs4 size 200

The following is a list of output messages from the **ping** command:

!	Success
-	Destination Host Unreachable
$	Invalid Host Address
X	TTL Expired in Transit
?	Unknown Host
*	Request Timed Out

The following is a list of available extended **ping** fields with descriptions:

Extended Commands	Specifies whether additional commands are desired for more ping configuration parameters. Answer yes (**y**) or no (**n**).
Source Address	Specifies the IPv4 address to use as the source address in the ECHO_REQ (or interface) packets.
Data Pattern	Specifies an alphanumerical string to use (the ASCII equivalent) as the data pattern in the ECHO_REQ packets.
Sweep Range of Sizes	Varies the sizes of the ECHO_REQ packets transmitted.
Sweep Min Size	Specifies the minimum size of the ECHO_REQ packet. Valid range is **0** to **65507**.
Sweep Max Size	Specifies the maximum size of the ECHO_REQ packet. Valid range is the sweep minimum size to **65507**.
Sweep Interval	Specifies the interval used to determine packet size when performing the sweep. Valid range is **1** to **65507**.
Verbose Output	Specifies an extended results output.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is an example of a successful **ping** command:

>**enable**
#ping


```
VRF Name [-default-]:
Target IP address:192.168.0.30
Repeat count [5]:5
Datagram Size [100]:100
Timeout in seconds [2]:2
Wait interval in milliseconds [100]:100
Extended Commands? [n]:n
Type CTRL+C to abort.
Legend: '!' = Success, '?' = Unknown host, '$' = Invalid host address
      '*' = Request timed out, '-' = Destination host unreachable
      'x' = TTL expired in transit, 'e' = Unknown error

Sending 5, 100-byte ICMP Echos to 192.168.0.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```


ping ethernet

Use the **ping ethernet** command to initiate a loopback message from one Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoint (MEP) to another MEP. These loopback messages are used to test the accessibility of the destination MEP. Variations of this command include:

ping ethernet <*target-mac-address* | *target-mep-id*>
ping ethernet <*target-mac-address* | *target-mep-id*> **count** <*number*>
ping ethernet <*target-mac-address* | *target-mep-id*> **data** <*pattern*>
ping ethernet <*target-mac-address* | *target-mep-id*> **domain** <*domain name*> **association** <*association name*>
ping ethernet <*target-mac-address* | *target-mep-id*> **domain none association** <*association name*>
ping ethernet <*target-mac-address* | *target-mep-id*> **drop-eligible**
ping ethernet <*target-mac-address* | *target-mep-id*> **interface** <*interface*>
ping ethernet <*target-mac-address* | *target-mep-id*> **mep** <*mep id*>
ping ethernet <*target-mac-address* | *target-mep-id*> **priority** <*priority*>
ping ethernet <*target-mac-address* | *target-mep-id*> **repeat** <*number*>
ping ethernet <*target-mac-address* | *target-mep-id*> **size** <*bytes*>
ping ethernet <*target-mac-address* | *target-mep-id*> **timeout** <*timeout*>
ping ethernet <*target-mac-address* | *target-mep-id*> **validate-data**
ping ethernet <*target-mac-address* | *target-mep-id*> **verbose**
ping ethernet <*target-mac-address* | *target-mep-id*> **wait** <*interval*>

After specifying the target for the loopback messages, the other parameters can be entered in any order.

Syntax Description

<*target-mac-address* | *target-mep-id*>	Specifies the destination for the loopback message. Medium access control (MAC) addresses are entered in the format **HH:HH:HH:HH:HH:HH**. Target MEP IDs are the unique numerical values identifying MEPs. MEP IDs range from **1** to **8191**.
count <*number*>	Optional. Specifies the number of loopback messages to send. Range is **1** to **1000000**.
data <*pattern*>	Optional. Specifies the pattern to be carried in the data time length value (TLV) of the loopback message. Pattern is up to four hexadecimal digits. Pattern range is **0** to **ffff**.
domain <*domain name*>	Optional. Specifies the maintenance domain to which the transmitting MEP belongs.
domain none	Optional. Specifies no maintenance domain.
association <*association name*>	Optional. Specifies the maintenance association to which the transmitting MEP belongs.

drop-eligible	Optional. Specifies the drop eligible bit value in the virtual local area network (VLAN) tag.
interface <*interface*>	Optional. Specifies the interface on which the transmitting MEP is configured. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.
mep <*mep id*>	Specifies the MEP ID of the transmitting MEP. MEP ID range is **1** to **8191**.
priority <*priority*>	Optional. Specifies the 802.1 priority bits that are sent in the loopback message. Range is **0** to **7**.
repeat <*number*>	Optional. Specifies the number of loopback messages to be sent. Range is **1** to **1024**.
size <*bytes*>	Optional. Specifies the size of the loopback message. Size ranges from **1** to **60** bytes.
timeout <*timeout*>	Optional. Specifies the time that the MEP will wait for a response to the loopback message. Range is **0** to **60** seconds.
validate-data	Optional. Specifies whether or not the transmitting MEP validates the contents of the data TLV in the received loopback messages.
verbose	Optional. Specifies that the results are in detailed, rather than summary, format.
wait <*interval*>	Optional. Specifies a minimum time to wait between sending loopback messages. Valid range is **100** to **60000** milliseconds.

Default Values

By default, the **count** value is set to **5**.

By default, the **data** pattern is set to **abcd**.

By default, the **drop-eligible** value is not set.

By default, the **interval** is set to **1000** milliseconds.

By default, the **priority** value is the priority specified in the MEP's configuration.

By default, the **size** value is set to **2** bytes.

By default, the **timeout** value is set to **2** seconds.

By default, the **validate-data** parameter is disabled.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface and the **wait** and **repeat** parameters.

Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

The **ping ethernet** command can be issued from both the Basic and Enable modes.

If the MEP ID is used as the target, the remote MEP must exist in the MEP continuity check message (CCM) database (meaning the remote MEP is transmitting valid CCMs) so that the MEP ID can be translated to the MAC address before the loopback message is transmitted.

Both the **domain** <*domain name*> and **association** <*association name*> parameters are not required if the source MEP ID of the MEP is specified and unique through the AOS device.

If the domain and association of the transmitting MEP are specified, and there is only one MEP in that domain or association, or if there is only one MEP configured on the unit, the **mep** <*mep id*> parameter is not required.

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

This command will not appear in the command line interface (CLI) unless Ethernet OAM CFM is enabled. To enable Ethernet OAM CFM, refer to the command *ethernet cfm on page 1273*.

Usage Examples

The following example initiates the Ethernet ping utility from an MEP in **Domain1** association **MA1** with a destination to an MEP with an MEP ID of **201**:

```
>enable
#ping ethernet 201 domain Domain1 association MA1
        Type CTRL+C to abort.
        Legend:    '!' = Success, '*' = Request timed out, 'd' = Data Mismatch
                   'o' = Out of order, '.' = No reply, 'e' = Unknown error.

        Sending 5, 100-byte LBRs to MEP 201 from MEP 1, timeout is 2 seconds:
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 202/668/1011 ms
```


ping ipv6

Use the **ping ipv6** command (at the Enable mode prompt) to verify IPv6 network connectivity. For information on how to verify IPv4 network connectivity, refer to *ping on page 512*. Variations of this command include:

ping [ipv6] <*ipv6 address*>
ping [ipv6] <*ipv6 address*> <*interface*>
ping [ipv6] <*ipv6 address*> **data** <*string*>
ping [ipv6] <*ipv6 address*> **destination-option**
ping [ipv6] <*ipv6 address*> **df-bit [0 |1]**
ping [ipv6] <*ipv6 address*> **dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]**
ping [ipv6] <*ipv6 address*> **hop-by-hop-option**
ping [ipv6] <*ipv6 address*> **repeat** <*number*>
ping [ipv6] <*ipv6 address*> **size** <*value*>
ping [ipv6] <*ipv6 address*> **source** <*ipv6 address*>
ping [ipv6] <*ipv6 address*> **mef-ethernet** <*slot/port*>
ping [ipv6] <*ipv6 address*> **system-control-evc**
ping [ipv6] <*ipv6 address*> **system-management-evc**
ping [ipv6] <*ipv6 address*> **timeout** <*value*>
ping [ipv6] <*ipv6 address*> **tos** <*value*>
ping [ipv6] <*ipv6 address*> **verbose**
ping [ipv6] <*ipv6 address*> **wait** <*interval*>
ping [ipv6] vrf <*name*> <*ipv6 address*>
ping [ipv6] vrf <*name*> <*ipv6 address*> <*interface*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **data** <*string*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **destination-option**
ping [ipv6] vrf <*name*> <*ipv6 address*> **df-bit [0 |1]**
ping [ipv6] vrf <*name*> <*ipv6 address*>**dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]**
ping [ipv6] vrf <*name*> <*ipv6 address*> **hop-by-hop-option**
ping [ipv6] vrf <*name*> <*ipv6 address*> **repeat** <*interval*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **size** <*value*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **source** <*ipv6 address*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **mef-ethernet** <*slot/port*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **system-control-evc**
ping [ipv6] vrf <*name*> <*ipv6 address*> **system-management-evc**
ping [ipv6] vrf <*name*> <*ipv6 address*> **timeout** <*value*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **tos** <*value*>
ping [ipv6] vrf <*name*> <*ipv6 address*> **verbose**
ping [ipv6] vrf <*name*> <*ipv6 address*> **wait** <*interval*>

After specifying the target IPv6 address to ping, the other parameters can be entered in any order. Use the **?** *after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

ipv6	Optional. Specifies an IPv6 ping.
<interface>	Specifies the egress interface when pinging an IPv6 link-local address (any address that has the prefix **FE80::/64**). Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ping ipv6** *<ipv6 address>* **?** to display a list of valid interfaces. This variable is mandatory when pinging a link-local address. This variable is ignored when using a non-link-local address.
<ipv6 address>	Specifies the IPv6 address of the system to ping. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. Entering the **ping ipv6** command using a link-local destination address prompts the user for an egress interface.
data *<string>*	Optional. Specifies an alphanumerical string to use (the ASCII equivalent) as the data pattern in the ICMPv6 ECHO_REQ packets.
destination-option	Optional. Includes the destination option in the ICMPv6 ECHO_REQ packets.
df-bit 0	Optional. Specifies that the Don't Fragment (DF) bit in the IP header is not set.
df-bit 1	Optional. Specifies setting the DF bit in the IP header. This will prevent the ping packets from being fragmented along the way.
dscp	Optional. Specifies the differentiated services code point (DSCP) value.
<value>	Optional. Valid range is decimal **0** to **63**. The value can also be specified in hexadecimal by adding a **0x** prefix to the number.
af*xx*	Optional. Specifies the assured forwarding (AF) class and subclass for the DSCP value. Select from: 11 (001010), 12 (001100), 13 (001110), 21 (010010), 22 (010100), 23 010110), 31 (011010), 32 (011100), 33 (011110), 41 (100010), 42 (100100), or 43 (100110).
cs*x*	Optional. Specifies the class selector (CS) value for the DSCP value. Valid range for *x* is **0** to **7**.
default	Optional. Specifies default (000000) DSCP value.
ef	Optional. Specifies expedited forwarding (EF) (101110) for the DSCP value.
hop-by-hop-option	Optional. Includes the hop-by-hop option in the ICMPv6 ECHO_REQ packets. This typically causes intermediate routers to process switch the packets, potentially detecting switching issues in these devices.
repeat *<number>*	Optional. Specifies the number of loopback messages to be sent. Range is **1** to **1024**.
size *<value>*	Optional. Specifies the datagram size (in bytes) of the ping packet. Valid range is **1** to **1448** bytes.

source <*ipv6 address*>	Optional. Specifies the IPv6 address to use as the source address in the ICMPv6 ECHO_REQ (or interface) packets. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. Entering the **ping ipv6** command using a link-local destination address prompts the user for an egress interface. The source IPv6 address must be a valid address local to the router on the specified virtual routing and forwarding (VRF) instance.
mef-ethernet <*slot/port*>	Optional. Specifies that the Metro Ethernet Forum (MEF) Ethernet interface is the ping target.
system-control-evc	Optional. Specifies that the system control Ethernet virtual connection (EVC) is the ping target.
system-management-evc	Optional. Specifies that the system management EVC is the ping target.
tc <*value*>	Optional. Specifies the traffic class (TC). The <*value*> can be specified as decimal **0** to **255**, or as hexidecimal
timeout <*value*>	Optional. Specifies the timeout period after which the ping is considered unsuccessful. Valid range is **1** to **60** seconds.
tos <*value*>	Optional. Specifies the type of service (ToS). The <*value*> can be specified as decimal (**0** to **255)** or as hexidecimal.
verbose	Optional. Enables detailed messaging.
vrf <*name*>	Optional. Specifies the VRF where the IPv6 address exists.
wait <*interval*>	Optional. Specifies a minimum time to wait between sending test packets. Valid range is **100** to **60000** milliseconds.

Default Values

By default, the **data** pattern is set to **abcd**.

By default, the **df-bit** is set to **0**.

By default, the **repeat** is set to **5**.

By default, the **size** value is set to **100** bytes.

By default, the **timeout** value is set to **2** seconds.

By default, the **wait** value is set to **100** milliseconds.

Command History

Release 18.1	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the **df-bit**, **dscp**, **system-control-evc**, **system-management-evc**, and **tos** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

The **ping ipv6** command can be issued from both the Basic and Enable modes.

The **ping ipv6** command helps diagnose basic IPv6 network connectivity using the Packet Internet Groper program to repeatedly bounce Internet Control Message Protocol version 6 (ICMPv6) ECHO_REQ packets off a system (using a specified IPv6 address). AOS allows executing a standard **ping ipv6** request to a specified IPv6 address, or provides keywords to configure a more specific **ping ipv6** configuration.

The following is a list of output messages from the **ping ipv6** command:

!	Success
-	Destination Host Unreachable
$	Invalid Host Address
x	TTL Expired in Transit
?	Unknown Host
*	Request Timed out
e	Unknown Error
B	Packet too Big

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example pings **2001:DB8:1A0::3** with **200** byte ICMPv6 ECHO_REQ packets:

```
>enable
#ping ipv6 2001:DB8:1A0::3 size 200
Type CTRL+C to abort.
Legend: '!' = Success, '?' = Unknown host, '$' = Invalid host address
      '*' = Request timed out, '-' = Destination host unreachable
      'x' = TTL expired in transit, 'e' = Unknown error
      'B' = Packet too big

Sending 5, 200-byte ICMP Echos to 2001:DB8:1A0::3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```


ping stack-member <*number*>

Use the **ping stack-member** command to ping a member of the stack. Variations of this command include:

ping stack-member <*number*>
ping stack-member <*number*> **vrf** <*name*>

Syntax Description

<*number*>	Specified which member of the stack to ping.
vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) where the stack-member exists.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

The **ping stack-member** command can be issued from both the Basic and Enable modes.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example pings a member of the stack:

```
>enable
#ping stack-member 3
Type CTRL+C to abort.
Legend: '!' = Success, '?' = Unknown host, '$' = Invalid host address
      '*' = Request timed out, '-' = Destination host unreachable
      'x' = TTL expired in transit
Sending 5, 100-byte ICMP Echos to 169.254.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2.2/3 ms
#
```


ping twamp

Use the **ping twamp** command to execute a Two-Way Active Measurement Protocol (TWAMP) type ping to measure the packet loss, delay, and interpacket delay variation (IPDV) and display the results of the test. Use the subcommands in any combination, in any order, when specifying the destination site. Variations of this command include:

ping twamp
ping twamp <*ip address* | *hostname*>
ping twamp <*ip address* | *hostname*> **control-port** <*port*>
ping twamp <*ip address* | *hostname*> **data pattern**
ping twamp <*ip address* | *hostname*> **data pattern ascii** <*pattern*>
ping twamp <*ip address* | *hostname*> **data pattern hex** <*pattern*>
ping twamp <*ip address* | *hostname*> **data random**
ping twamp <*ip address* | *hostname*> **data zero**
ping twamp <*ip address* | *hostname*> **dscp** <*value*>
ping twamp <*ip address* | *hostname*> **interval** <*value*>
ping twamp <*ip address* | *hostname*> **port** <*port*>
ping twamp <*ip address* | *hostname*> **repeat** <*value*>
ping twamp <*ip address* | *hostname*> **size** <*value*>
ping twamp <*ip address* | *hostname*> **source** <*ip address*>
ping twamp <*ip address* | *hostname*> **source-port** <*port*>
ping twamp <*ip address* | *hostname*> **timeout** <*value*>
ping twamp <*ip address* | *hostname*> **verbose**
ping twamp <*ip address* | *hostname*> **wait** <*value*>
ping twamp vrf <*name*>
ping twamp vrf <*name*> <*ip address* | *hostname*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **control-port** <*port*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **data pattern**
ping twamp vrf <*name*> <*ip address* | *hostname*> **data pattern ascii** <*pattern*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **data pattern hex** <*pattern*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **data random**
ping twamp vrf <*name*> <*ip address* | *hostname*> **data zero**
ping twamp vrf <*name*> <*ip address* | *hostname*> **dscp** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **interval** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **port** <*port*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **repeat** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **size** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **source** <*ip address*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **source-port** <*port*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **timeout** <*value*>
ping twamp vrf <*name*> <*ip address* | *hostname*> **verbose**

ping twamp vrf <*name*> <*ip address* | *hostname*> **wait** <*value*>

*The subcommands can be used in a string of any available combination. Use the **?** after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

<*ip address* | *hostname*>	Optional. Specifies the IP address or host name of the system to ping. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Entering the **ping twamp** command with no specified IP address prompts the user with parameters for a more detailed **ping twamp** configuration.
control-port <*port*>	Optional. Specifies the destination TWAMP control port. Port range is **1** to **65535**.
data	Optional. Specifies data used to pad packets. The following options are available:
pattern	Pads the packet with a user-specified pattern.
ascii <*pattern*>	Pads the packet with a user-specified ascii pattern.
hex <*pattern*>	Pads the packet with a user-specified hex pattern.
random	Pads the packet with random numbers.
zero	Pads the packet with all zeros.
dscp <*value*>	Optional. Specifies the differentiated services code point (DSCP) value. Valid range is **0** to **63**.
interval <*value*>	Optional. Specifies the interval between consecutive ping TWAMPs (in milliseconds). Valid range is **5** to **5000**.
port <*port*>	Optional. Specifies the destination port for the TWAMP test packets. Valid range is **1** to **65535**.
repeat <*value*>	Optional. Specifies the number of ping TWAMP packets. Valid range is **1** to **1000**.
size <*value*>	Optional. Specifies the datagram size. Valid range is **0** to **1462**.
source <*ip address*>	Optional. Specifies the source IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
source-port <*port*>	Optional. Specifies the source port for the TWAMP test packets. Valid range is **1** to **65535**.
timeout <*value*>	Optional. Specifies the timeout value in milliseconds. Valid range is **100** to **60000**.
verbose	Optional. Displays the detailed two-way ping verbose results for the specified IP address or host name.
vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) instance within which the ping is executed. If no VRF is specified, the default (unnamed) VRF is used.

wait <*value*>	Optional. Specifies the interval (in milliseconds) between consecutive TWAMP test packets. Range is **5** to **5000**.

Default Values

By default, the **data** is **zero,** the **dscp** is **0**, the **interval** value is **20,** the **port** value is **0,** the repeat value is **100**, the **size** is **0**, and the **timeout** is **2000** milliseconds.

Command History

Release 17.4	Command was introduced to replace the **twping** command.
Release 17.6	Command was expanded to include **control-port** and **wait** keywords.
Release A4.01	Command was expanded to include the **ascii** and **hex** pattern parameters.
Release R11.2.0	Command was expanded to include the **vrf** parameter.

Functional Notes

The **ping twamp** command can be issued from both the Basic and Enable modes.

Usage Examples

The following example executes a TWAMP ping:

```
>enable
#ping twamp
2009.06.03 11:18:24 IP.TWPING CTRL EVNT Attempting to connect
2009.06.03 11:18:24 IP.TWPING CTRL EVNT State changed Init -> Opening (event=Open Connection)
2009.06.03 11:18:24 IP.TWPING CTRL EVNT State changed Opening -> Setup (event=RX
    Server-Greeting)
2009.06.03 11:18:24 IP.TWPING CTRL EVNT State changed Setup -> Starting (event=TX
    Setup-Response)
2009.06.03 11:18:24 IP.TWPING CTRL PKT Sending Setup-Response (len=140)
 mode=1
 keyId=00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--MORE--
```

port-auth re-authenticate

Use the **port-auth re-authenticate** command to force the reauthentication of every currently authorized host on all interfaces in the AOS unit. Variations of this command include:

port-auth re-authenticate
port-auth re-authenticate <*interface*>

Syntax Description

<*interface*>	Optional. Specifies reauthentication of a specific interface. Interfaces are specified in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **port-auth re-authenticate ?** for a complete list of available interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example specifies that the authorized hosts on the interface **eth 1/1** are reauthenticated:

>enable
#port-auth re-authenticate eth 1/1

ramdisk <*size*>

Use the **ramdisk** command to create a volatile RAM disk file system and allocate memory in bytes to the newly created RAM disk. Use the **no** form of this command to delete the RAM disk.

*Not all units are capable of using a RAM disk file system. Use the **?** command to display a list of valid commands at the enable prompt.*

Syntax Description

<*size*>	Specifies the size of the RAM disk in bytes. Valid range is **65536** to the maximum available heap size on the unit. Input for this value allows the use of the following characters as multipliers: **M**, **m**, **K**, and **k**.

Default Values

No default values are necessary for this command.

Command History

Release 17.7	Command was introduced.

Usage Examples

The following example creates a volatile RAM disk file system and allocates **128000** bytes of memory:

```
>enable
#ramdisk 128000
```

The following example creates a volatile RAM disk file system and uses the multiplier **k** to allocate 131072 bytes of memory (where **128k** is 128 x 1024 = 131072):

```
>enable
#ramdisk 128k
```

reload

Use the **reload** command to perform a manual reload of AOS. Variations of this command include:

reload
reload cancel
reload hard
reload in <*delay*>
reload soft
reload vcid <*vcid*>

*Performing an AOS **reload** disrupts data traffic.*

Syntax Description

cancel	Optional. Deactivates a pending **reload** command.
hard	Optional. Performs a hard reload.
in <*delay*>	Optional. Specifies a delay period in minutes (mm) or hours and minutes (hh:mm) that AOS will wait before reloading.
soft	Optional. Performs a soft reload.
vcid <*vcid*>	Optional. Specifies an ActivChassis member to reload. Valid range is **1** to **8**. VCID values **1** and **2** are for the master and backup device, respectively. The VCID of the current master device will not be accepted.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release AC1.0	Command was expanded to include the **vcid** parameter.
Release R10.10.0	Command was expanded to include the **hard** and **soft** parameters.

Usage Examples

The following example reloads the AOS software in 3 hours and 27 minutes:

>**enable**
#reload in 03:27

The following example reloads the AOS software in 15 minutes:

>**enable**
#reload in 15

The following example terminates a pending reload command:

>**enable**
#reload cancel

The following example reloads ActivChassis member **3**:

>**enable**
#reload vcid 3

reload dot11 interface dot11ap *<ap interface>*

Use the **reload dot11 interface dot11ap** command to perform a cold start of a wireless access point (AP) that is currently controlled by the wireless access controller (AC) on which the command is executed. Variations of this command include:

reload dot11 interface dot11ap *<ap interface>*
reload dot11 interface dot11ap *<ap interface>* **factory-default**

Syntax Description

<ap interface>	Specifies the AP interface number to reload. Range is **1** to **8**.
factory-default	Optional. Specifies reloading the unit with the factory default settings.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example performs a cold start for AP interface 1:

```
>enable
#reload dot11 interface dot11ap 1
AP 1 reloaded
Router#
2006.12.23 19:14:03 DOT11.Session : AP 1: AP reboot.
2006.12.23 19:14:03 DOT11.Session : AP 1: Control session lost.
2006.12.23 19:14:03 DOT11.Session : AP 1: Control session established.
```


rename

Use the **rename** command to rename a file stored in the AOS product. Variations of this command include:

rename <*source filename*> <*destination filename*>
rename cflash <*source filename*> <*destination filename*>
rename flash <*source filename*> <*destination filename*>
rename usbdrive0 <*source filename*> <*destination filename*>

Syntax Description

cflash	Optional. Specifies the file to be renamed is on the Compact flash drive.
flash	Optional. Specifies the file to be renamed is on the flash drive.
usbdrive0	Optional. Specifies the file to be renamed is on the Universal Serial Bus (USB) drive.
<*source filename*>	Specifies the file to be renamed.
<*destination filename*>	Specifies the new name of the file.

Default Values

No default values are necessary for this command.

Command History

Release R10.10	Command was introduced.

Functional Notes

If no drive is specified (**cflash**, **flash**, or **usbdrive0**), this command is executed in the first mounted drive.

An error is displayed if you attempt rename the file with the same name, or if a file by the destination filename already exists.

Files cannot be renamed from one file system to another. For example, a file in flash cannot be renamed in Cflash).

Usage Examples

The following example renames the file **File1** in the flash drive to **File3**:

>**enable**
#rename flash File1 File3

run audit security

Use the **run audit security** command to run a security audit on the AOS device. Variations of this command include:

run audit security
run audit security log
run audit security log cflash
run audit security log usbdrive0

Once the audit is in process, the session will be blocked until the audit is completed or until Ctrl+C is issued.

Syntax Description

cflash	Optional. Specifies saving the log file to CompactFlash® memory.
log	Optional. Specifies saving the audit results to a file named **securityAudit_**<*timestamp*>. The file name has the timestamp attached in the format yyyymmddhhmmss. If **cflash** is not specified, the file is saved to flash memory.
usbdrive0	Optional. Specifies saving the log file to Universal Serial Bus (USB) flash drive memory.

Default Values

No default values are necessary for this command.

Command History

Release 17.7	Command was introduced.
Release 18.2	Command was expanded to include the **usbdrive0** parameter.

Functional Notes

The security audit tool is used to identify possible security violations. The results of the audit can be viewed by using the **show audit security** command (refer to *show audit security on page 552*), or by viewing the log file using the commands *show flash on page 653* or *show cflash on page 580*.

The **show audit security** command displays a summary of the security audit results including: the type of defect, severity, and a brief description. The **show audit security detail** command lists the summary, as well as details of the defect and recommends corrective action. It is up to the customer to determine if the findings are a true risk in their system, and to make the necessary adjustments to their configuration. Some items could be recorded as possible risks that are not actual risks based on the entire network configuration.

If two people are logged in simultaneously (for example, one via Telnet and one via the console) and both try to run the audit security tool, the user who begins the audit first will take precedence. An error message will be displayed to the second user that an audit is in progress.

The following table lists the configuration items that are audited for security risks.

Violation Type	Severity	Description
Startup-Config	High	Indicates that the startup configuration file does not match the running configuration file. This is determined by comparing the MD5 checksum of both files for a match.
Passwords/Keys	High	Identifies nonsecure passwords. If a password has MD5 encryption enabled, the tool tests for common password sequences, such as qwerty, 1234, abc, xyz, etc. If MD5 is disabled, an alert is issued if the password: • Is less than 7 characters. • Does not contain alphabetic and numeric characters. • Matches common sequences, such as qwerty, 1234, abc, xyz, etc. • Matches the default passwords. • Matches another password in the system. • Service password encryption is not enabled.
Firewall	High	Indicates the firewall is disabled.
Policy-Class	High	Identifies any of the following access control policy (ACP) vulnerabilities: • Stateful inspection is disabled. • An undefined access control list (ACL) exists in the ACP. • An interface with a private IP address (10.x.x.x, 172.16.x.x, 192.168.x.x) has an ACP assigned that does not have NAT configured. • An interface is enabled without an ACP assigned.
SNMP	High	Indicates the SNMP agent is enabled and configured to allow SNMPv1 or SNMPv2. Both of these versions are considered nonsecure. SNMPv3 group and SNMPv3 user are preferred.
Network Protocols	High	Identifies any of the following network protocols are enabled and considered a security risk: HTTP, HTTPS SSLv2, FTP, TFTP, and Telnet. SSH is suggested as a replacement for Telnet and HTTPS SSLv3 instead of HTTPS SSLv2.

Violation Type	Severity	Description
WIFI	High	Identifies any of the following wireless vulnerabilities: • Security mode is set to anything but WPA2 (including none). • Service set identifier (SSID) broadcast is enabled. • A weak key.
Session Timeout	High	Identifies the console, HTTP, SSH, or Telnet session timeout is set to a value greater than 15 minutes. Long session timeouts can compromise the system. The recommended setting is 15 minutes or less.
Time-Server	High	Indicates the time server (SNTP or NTP) is not configured or is configured but not synchronized. It is important to have a valid timestamp on all logs generated by the system.
Logging	Medium	Indicates user activity is not being logged. User activity should be logged either by enabling syslog or TACACS+ accounting. (The syslog can be enabled by using the **logging forwarding on** command.)
Domain Lookup	Medium	Indicates **domain-lookup** is enabled but a DNS server has not been configured. This allows DNS requests to be broadcast.
Interfaces	Medium	Identifies the following interface vulnerabilities: • The **ip directed-broadcast** is enabled which could make an interface vulnerable to denial of service attacks. • A static ACL assigned to an interface. A more secure option is to enable the firewall and assign an ACP.
Enable Password	Low	Indicates the enable password is not set for MD5 encryption. MD5 encryption is more secure than standard password encryption.
Banner	Low	Indicates the default executive banner is still set. It is recommended that a custom banner be displayed when a user attempts to login. The banner warns of the legal consequences of unauthorized access to the unit.
TCL Scripts	Low	Indicates Tcl scripting is enabled. Scripts could cause damage to configuration of the unit.

Usage Examples

The following example initiates the security audit and saves the results to a log file in flash memory:

>**enable**
#run audit security log
Audit Complete

run checkdisk cflash

Use the **run checkdisk cflash** to run checkdisk to check and fix file system errors. This command should only be issued promptly after system reboot while voicemail processes are idle. Issuing the command while voicemail processes are active could result in file system corruption.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.03	Command was introduced.

Usage Examples

The following example checks and fixes file system errors:

```
>enable
#run checkdisk cflash
```

run checkdisk usbdrive0

Use the **run checkdisk usbdrive0** to run checkdisk to check and fix file system errors on the Universal Serial Bus (USB) drive. Variations of this command include:

run checkdisk usbdrive0
run checkdisk usbdrive0 dontfix

Syntax Description

dontfix	Specifies the unit to run checkdisk on the USB flash drive without fixing errors.

Default Values

No default values are necessary for this command.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example checks and fixes file system errors on the USB flash drive:

>**enable**
#run checkdisk usbdrive0

run tcl *<name>*

Use the **run tcl** command to initiate a tool command language (Tcl) script.

Syntax Description

<name>	Specifies the name of the Tcl script file or inline Tcl script to run.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release R11.1.1	Command was expanded to include inline scripts.

Usage Examples

The following example initiates the **test1.tcl** Tcl script file:

```
>enable
#run tcl test1.tcl

Script execution complete

#
```

run voipwizard

Use the **run voipwizard** command to run the Voice over IP (VoIP) Setup Wizard. This wizard configures the basic settings for running VoIP applications on switchports. After running the wizard, you can view the log file using the command *show voipwizard log on page 1111*.

> NOTE *The wizard changes the current configuration of the unit. If the unit has already been configured, the changes could conflict with current settings. You will be able to review the changes before applying them to the system.*

Syntax Description

No subcommands.

Default Values

There is no default setting for this command.

Command History

Release R11.3.0	Command was introduced.

Functional Notes

When running the VoIP Setup Wizard, you are given the option of applying the recommended settings or specifying your own settings. If you enter **yes** to accept the recommended settings, the wizard will configure the settings and ask for confirmation before applying them.

If you choose to specify your own settings instead of applying the recommendations, enter **no**, and the wizard will step you through the different setting options as shown in the following example:

```
>enable
#run voipwizard

Welcome to the VoIP Configuration Wizard.

This wizard will assist you in configuring your NetVanta 1234 for
switching. You may automatically apply Adtran's recommended VoIP settings or
specify your own port assignments.

WARNING: This will change the current configuration of the unit. If this unit
has already been configured, the following changes may conflict with the
current settings. You will be able to review your changes before they are
applied.

Adtran VoIP Recommendation:

Ports assigned as voice ports: (switchport 0/1-24)
Ports assigned as uplink ports: (gigabit-switchport 0/1-4)
```


Voice port configuration: description voice
spanning-tree edgeport
no shutdown
switchport voice vlan 2
qos trust cos

Uplink port configuration: description uplink
no shutdown
switchport mode trunk
qos trust cos

Global QoS configuration: qos queue-type wrr 25 25 25 expedite
qos cos-map 1 0 1
qos cos-map 2 2 4
qos cos-map 3 3 6
qos cos-map 4 5 7

Would you like to apply this recommendation? [yes/no]

no

What would you like to use as your voice vlan? (1-4094) [default: 2]

2

What are the types of interfaces you would like to configure as voice ports?

--- Options ---
1. switchport
2. gigabit-switchport

[default: switchport]

Specify one or more port types. (Examples: 1,2,1-2)
Enter your selection:

1
Selected: switchport

For the 'switchport' interface type, which ports would you like to
assign as voice ports? Enter port numbers or ranges of port numbers separated
by commas. (Example: 1,2,3-9,13,15) [default: 1-24]

1-24

What are the types of interfaces you would like to configure as uplink ports?

--- Options ---

1. switchport
2. gigabit-switchport

[default: gigabit-switchport]

Specify one or more port types. (Examples: 1,2,1-2)
Enter your selection:

2

Selected: gigabit-switchport

For the 'gigabit-switchport' interface type, which ports would you like to
assign as uplink ports? Enter port numbers or ranges of port numbers separated
by commas. (Example: 1,2,3-9,13,15) [default: 1-4]

1-4

Would you like to enable port security on all voice ports?
(yes/no) [default: no]

yes

How many mac addresses would you like to allow on each voice
port? (1-132) [default: 2]

2

Selected VoIP configuration:

Ports assigned as voice ports: (switchport 0/1-24)
Ports assigned as uplink ports: (gigabit-switchport 0/1-4)

Voice port configuration: description voice
spanning-tree edgeport
no shutdown
switchport voice vlan 2
qos trust cos
switchport port-security
switchport port-security maximum 2

Uplink port configuration: description uplink
no shutdown
switchport mode trunk
qos trust cos

Global QoS configuration: qos queue-type wrr 25 25 25 expedite
qos cos-map 1 0 1


```
qos cos-map 2 2 4
qos cos-map 3 3 6
qos cos-map 4 5 7
```

Would you like to apply this configuration? [yes/no]

yes

Saving configuration...
Configuration successfully saved!

Thank you for using the VoIP Configuration Wizard.
Goodbye.

Script execution complete

Usage Examples

The following example initiates the VoIP Setup Wizard:

>**enable**
#run voipwizard

show activchassis

Use the **show activchassis** command to display information about ActivChassis members. Variations of this command include:

show activchassis
show activchassis detail
show activchassis <*vcid*>
show activchassis <*vcid*> **detail**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

detail	Optional. Specifies that detailed ActivChassis information is displayed, including the ActivChassis ID (VCID), the connection state, and the role of the member, as well as additional information.
<*vcid*>	Optional. Specifies that information about a specific ActivChassis member is displayed. VCID range is **1** to **8**. VCID values of **1** and **2** are given to the master and backup devices, respectively.

Default Values

No default values are necessary for this command.

Command History

Release AC1.0	Command was introduced.

Functional Notes

This command is available from both the ActivChassis master and linecard devices' CLI. In the linecard command mode, only the master and linecard ActivChassis members are displayed. If the linecard has not been admitted to the ActivChassis, the command only displays the linecard information.

For more information about the difference between linecard and master devices, and how to access the CLI for each, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example displays detailed information about all ActivChassis members:

>**enable**
#show activchassis detail
VCID: 1 (NV1638)
ActivChassisVC Connection State: Connected
Role: Master
Connection Information: none
ActivChassisVC Ports:
  Xgiga-switchport 1/1/1
  Xgiga-switchport 1/1/2

VCID: 4 (NV 1638)
ActivChassisVC Connection Sate: Not Connected
Role: Linecard
Connection Information: “This device has the wrong AOS version. The correct version is AC1.0.”
ActivChassisVC Ports:
  Xgiga-switchport 4/0/1
  Xgiga-switchport 4/0/1

show arp

Use the **show arp** command to display the Address Resolution Protocol (ARP) table. Variations of this command include:

show arp
show arp realtime
show arp vrf <*name*>
show arp vrf <*name*> **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance or your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.
vrf <*name*>	Optional. Displays information only for the specified virtual routing and forwarding (VRF). If a VRF is not specified, the default VRF is assumed.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **show arp** command:

```
>enable
#show arp
ADDRESS         TTL(min)    MAC ADDRESS        INTERFACE    TYPE
10.22.18.3      19          00:E0:29:6C:BA:31  eth 0/1      Dynamic
192.168.20.2    16          00:A0:C8:0D:E9:AD  eth 0/2      Dynamic
224.0.0.5       20          01:00:5E:00:00:05  eth 0/2      Permanent
```


show as-path-list

Use the **show as-path-list** command to display any AS path lists that have been configured in the router, along with any permit and deny clauses in each list. Variations of this command include:

show as-path-list
show as-path-list *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Optional. Specifies that the command display only the list matching the specified AS path list name. If not specified, all AS path lists are displayed.

Default Values

By default, this command displays all AS path lists.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R10.1.0	Command syntax was changed and the **ip** keyword was removed for all AOS products.

Usage Examples

In the following example, all AS path lists defined in the router are displayed.

```
>enable
#show as-path-list
as-path-list AsPathList1:
 permit 100
 permit 200
 permit 300
 deny 6500
as-path-list AsPathList2:
 permit 400
 permit 500
```


show atm pvc

Use the **show atm pvc** command to display information specific to the asynchronous transfer mode (ATM) interface's permanent virtual circuit (PVC). Variations of this command include the following:

show atm pvc
show atm pvc interfaces atm <*interface*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interfaces atm <*interface*>	Optional. Displays the ATM PVC information for a specific PVC. Specify an ATM interface (valid range is **1** to **1023**) or a subinterface in the format <*interface id.subinterface id*> (for example, **1.1**). Using this command without specifying an interface will display all information for all ATM PVCs.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show atm pvc interfaces** command:

```
>enable
#show atm pvc interface atm 1.1
```

Name	VPI	VCI	Encap Type	SC	Peak Kbps	Avg/Min Kbps	Burst Cells	Status
atm 1.1	0	200	SNAP	N/A	0	0	0	Active

show atm traffic interface atm <*interface*>

Use the **show atm traffic interface atm** command to display traffic information specific to the asynchronous transfer mode (ATM) interface.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Specifies an ATM port number. Specify an ATM interface (valid range is **1** to **1023**) or a subinterface in the format *<interface id.subinterface id>* (for example, **1.1**).

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show atm traffic** command from ATM interface 1:

```
>enable
#show atm traffic interface atm 1
atm 1 is UP, line protocol is UP
 BW 896 Kbit/s
 16 maximum active VCCs, 16 VCCs per VP, 1 current VCCs
Queueing strategy: Per VC Queueing
 5 minute input rate 32 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
    19 packets input, 1357 bytes
    0 pkts discarded, 0 error pkts, 0 unknown protocol pkts
    45 cells received, 0 OAM cells received
    0 packets output, 0 bytes
    0 tx pkts discarded, 0 tx error pkts 0 internal tx error pkts
    0 cells sent, 0 OAM cells sent
```


The following is sample output from the **show atm traffic** command from ATM subinterface 1.1:

#show atm traffic interface atm 1.1
27 Input Packets
0 Output Packets
72 Cells received, 0 OAM cells received
F5 InEndLoopReq: 0 F5 InEndLoopResp: 0 F5 InAIS: 0 F5 InRDI: 0
0 Cells sent, 0 OAM cells sent
F5 OutEndLoopReq: 0 F5 OutEndLoopResp: 0 F5 OutAIS: 0 F5 OutRDI: 0
0 OAM Loopback Successes 0 OAM Loopback Failures

show audit security

Use the **show audit security** command to display the results of the security audit including: the type of defect, severity, and a brief description. The security audit must be initiated first using the command *run audit security on page 534*. Variations of this command include:

show audit security
show audit security detail

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Optional. Displays the details of the security audit and recommends corrective action.

Default Values

No default values are necessary for this command.

Command History

Release 17.7	Command was introduced.

Functional Notes

The security audit tool is used to identify possible security violations and is initiated by using the command *run audit security on page 534*.

The **show audit security detail** command lists a summary of the results, as well as details of the defect and recommends corrective action. It is up to the customer to determine if the findings are a true risk in their system, and to make the necessary adjustments to their configuration. Some items could be recorded as possible risks that are not actual risks based on the entire network configuration.

Usage Examples

The following is sample output from the **show audit security** command:

>enable
#show audit security
Using 2214 bytes

SUMMARY

Severity	Type	Description
LOW	Enable Password	MD5 encryption is not enabled
HIGH	Network Protocol	FTP server enabled
HIGH	Network Protocol	TFTP server enabled
HIGH	Network Protocol	HTTP server enabled
HIGH	Network Protocol	Telnet enabled
HIGH	Policy-Class	Private, undefined ACL
HIGH	Policy-Class	Private, stateless
HIGH	Policy-Class	Public, stateless
HIGH	Policy-Class	Public, NAT not enabled
HIGH	Policy-Class	Interfaces using default policy-class
HIGH	Password	Weak Passwords
HIGH	Password	Duplicate Passwords
HIGH	Session Timeout	Console timeout >= 15 minutes
HIGH	Session Timeout	Telnet 0 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 1 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 2 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 3 timeout >= 15 minutes
HIGH	Session Timeout	Telnet 4 timeout >= 15 minutes
HIGH	Session Timeout	SSH 0 timeout >= 15 minutes
HIGH	Session Timeout	SSH 1 timeout >= 15 minutes
HIGH	Session Timeout	SSH 2 timeout >= 15 minutes
HIGH	Session Timeout	SSH 3 timeout >= 15 minutes
HIGH	SNMP	Using SNMPv1/v2, not secure

The following is sample output from the **show audit security detail** command:

>**enable**
#show audit security detail
Using 4193 bytes

DETAIL

ENABLE PASSWORD:

* The enable password is not set for MD5 encryption. MD5 encryption is more secure than standard password encryption.

NETWORK PROTOCOLS:

* The following protocols are enabled and may be a security risk.
Disable if not needed. Use SSH instead of Telnet and HTTP SSLv3 instead of
HTTP SSLv2.

  * FTP
  * TFTP
  * HTTP
  * Telnet

POLICY-CLASS:

---

* Potential vulnerabilities were found with the following policies. Note: NAT
may not be required on all policies; however, broadcast of IP addresses from the
internal network to the Internet should be restricted. This tool did not take
into account how the policies are used. Depending upon the configuration of your
network, these policies may or may not make your network vulnerable.

****

Name	Line	Description
**********		
Private	2	Allows undefined ACL
Private	3	Allows stateless-inspection
Public	4	Allows stateless-inspection
Public	N/A	NAT not enabled for Private interface, eth 0/1

* The following interfaces are enabled but do not have a policy-class
assigned. Not having a policy-class assigned will leave the interface open to
attack.

  * vlan 1210

PASSWORDS / KEYS:

---

* Passwords should be at least 7 characters and have both alphabetic and
numeric characters. Some passwords are considered weak if they match default
passwords or contain common sequences. For example Qwerty123 is considered a
weak password even though it contains both numeric and alphabetic characters.
The following weak passwords were found:

  * 1f1965f156e907907d3a8ed5172557a86736(encrypted)
  * 2b2d9aa78c8dfb9fca1cf745d72e2e28cc99(encrypted)
  * 373fbaa34722617409e24b9d9a707cb09fe3(encrypted)
  * 1610d7b313a09983a2de5bb4f1a77997f346(encrypted)
  * 24223699587eef35644778c8a901cca82a70(encrypted)
  * 46400f529e54aeb56fa224fadb14c111f007(encrypted)

* Each user should have a unique password. The following passwords
are duplicated:

  * 2b2d9aa78c8dfb9fca1cf745d72e2e28cc99(encrypted)
  * 46400f529e54aeb56fa224fadb14c111f007(encrypted)

SESSION TIMEOUT:

---

* The following sessions have timeout values of 15 minutes or greater. Long
session timeouts may allow your system to be compromised. To increase
security, set the timeout value to less than 15 minutes.
* Console
  * Telnet 0
  * Telnet 1
  * Telnet 2
  * Telnet 3
  * Telnet 4
  * SSH 0
  * SSH 1
  * SSH 2
  * SSH 3

SNMP:

---

* The SNMP agent is enabled and is configured to allow SNMPv1 and
SNMPv2 which are not secure. If SNMP is needed, remove the community
names and add SNMPv3 group and SNMPv3 user.

---

show auto-config

Use the **show auto-config** command to display the AOS automatic self-configuration feature status and settings.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R10.5.0	Output was expanded to include the cause of the last failure.

Usage Examples

The following is sample output from the **show auto-config** command:

```
>enable
#show auto-config
Auto-Config is enabled, current status: Downloading.
File transfer method is TFTP
Config Server is 10.10.10.1
Config filename is Adtran_CONFIG.cfg
Default filename is [00A0C8AE103A.cfg | adtran_4700254F2.cfg |
adtran_000000000000.cfg], Current: (Disabled)
Maximum retry count is 0 (repeat indefinitely), total retries is 0
Last failure: HTTP: Could not send initial message to HTTP server
```


show auto-link

Use the **show auto-link** command to display the auto-link feature configuration and current status.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.3/A2	Command was introduced.

Usage Examples

The following is sample output of the **show auto-link** command:

```
>enable
#show auto-link
Auto-link: Enabled
   Use Http: Enabled
   Server URL: 10.14.1.55/aps/DiscoveryProcessor?action=devinfo
   Server SERVER: 10.14.1.55
   Recontact Interval: 3600 seconds
   Last Contact: Tue, June 17, 2008 10:32:01 AM
   Next Contact: Tue, June 17, 2008 11:30:23 AM
   Status: Discovered
```


show battery

Use the **show battery** command to display battery information. Variations of this command include:

show battery
show battery <*slot/port*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*slot/index*>	Optional. Specifies the slot and port of the battery information in the format <*slot/port*>, for example, **0/1**.

Default Values

No default values are necessary for this command.

Command History

Release R11.10.0	Command was introduced.
Release R11.11.0	Command output options were altered and noted in the Functional Notes section.

Functional Notes

The output information displays the battery status **Good**, **Failure**, **Charging**, **Unknown**, **Not Connected**, or **Low**. The current power source displays either **AC** or **Battery**, indicating where the unit is currently sourcing power.

Usage Examples

The following example displays battery information for slot **0**, port **1**:

>enable
#show battery 0/1

```
Battery 0/1 Information
===========================
Battery Status          : Good
Current Power Source    : AC
Battery Install Date    : June 12 2015, 12:40:34
```


show bgp

Use the **show bgp** command to display details about Border Gateway Protocol (BGP) configuration on the AOS device, including the specified route, advertising router IPv4 or IPv6 address, router ID, and the list of neighbors to which this route is being advertised. Variations of this command include:

show bgp any-vrf ipv4
show bgp any-vrf ipv4 *<ipv4 address>*
show bgp any-vrf ipv4 *<ipv4 address> <subnet mask>*
show bgp any-vrf ipv4 summary
show bgp ipv4
show bgp ipv4 *<ipv4 address>*
show bgp ipv4 *<ipv4 address> <subnet mask>*
show bgp ipv4 summary
show bgp vrf *<name>* **ipv4**
show bgp vrf *<name>* **ipv4** *<ipv4 address>*
show bgp vrf *<name>* **ipv4** *<ipv4 address> <subnet mask>*
show bgp vrf *<name>* **ipv4 summary**
show bgp any-vrf ipv6
show bgp any-vrf ipv6 *<ipv6 address/prefix-length>*
show bgp any-vrf ipv6 summary
show bgp ipv6
show bgp ipv6 *<ipv6 address/prefix-length>*
show bgp ipv6 summary
show bgp vrf *<name>* **ipv6**
show bgp vrf *<name>* **ipv6** *<ipv6 address/prefix-length>*
show bgp vrf *<name>* **ipv6 summary**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

any-vrf	Optional. Displays BGP information for all virtual routing and forwarding (VRF) instances.
ipv4	Displays IPv4 BGP route information.
ipv6	Displays IPv6 BGP route information.
vrf *<name>*	Optional. Displays BGP information for a specific VRF instance.
<ipv4 address>	Optional. Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

<subnet mask>	Optional. Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
<ipv6 address/prefix-length>	Optional. Specifies a valid IPv6 address and prefix. IPv6 addresses should be expressed in colon hexadecimal format (for example, **2001:DB8:3F::/48**).
summary	Optional. Displays the status of all BGP connections.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products. Command was also expanded to include the **any-vrf**, **ipv4**, and **vrf** <*name*> parameters.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products. Command was also expanded to include the **ipv6** and <*ipv6 address/prefix-length*> parameters.

Usage Examples

The following sample output of the **show bgp ipv4 summary** command shows a summarized list of the configured BGP neighbors, as well as their status and statistics.

>**enable**
#show bgp ipv4 summary
BGP router identifier 192.168.3.1, local AS number 304
8 network entries, 5 paths, and 23 BGP path attribute entries

Neighbor	V	AS	MsgRcvd	MsgSent	InQ	OutQ	Up/Down	State/PfxRcd
10.22.131.1	4	302	95	104	0	0	01:30:06	9
10.22.131.9	4	302	97	105	0	0	01:30:07	21
10.22.132.9	4	303	200	179	0	0	02:43:09	21
10.22.134.1	4	304	166	178	0	0	02:43:15	3
10.22.134.10	4	304	174	179	0	0	02:43:24	7
10.22.134.26	4	304	172	174	0	0	02:41:43	10
10.22.134.34	4	304	164	174	0	0	02:41:40	4

show bgp community

Use the **show bgp community** command to display only those routes learned using Border Gateway Protocol (BGP) that match the community numbers specified in the command. If no communities are specified, all BGP routes containing a community attribute are shown. Variations of this command include:

show bgp any-vrf ipv4 community
show bgp any-vrf ipv4 community <*number*>
show bgp any-vrf ipv4 community exact
show bgp any-vrf ipv4 community internet
show bgp any-vrf ipv4 community local-as
show bgp any-vrf ipv4 community no-advertise
show bgp any-vrf ipv4 community no-export
show bgp ipv4 community
show bgp ipv4 community <*number*>
show bgp ipv4 community exact
show bgp ipv4 community internet
show bgp ipv4 community local-as
show bgp ipv4 community no-advertise
show bgp ipv4 community no-export
show bgp vrf <*name*> **ipv4 community**
show bgp vrf <*name*> **ipv4 community** <*number*>
show bgp vrf <*name*> **ipv4 community exact**
show bgp vrf <*name*> **ipv4 community internet**
show bgp vrf <*name*> **ipv4 community local-as**
show bgp vrf <*name*> **ipv4 community no-advertise**
show bgp vrf <*name*> **ipv4 community no-export**
show bgp any-vrf ipv6 community
show bgp any-vrf ipv6 community <*number*>
show bgp any-vrf ipv6 community exact
show bgp any-vrf ipv6 community internet
show bgp any-vrf ipv6 community local-as
show bgp any-vrf ipv6 community no-advertise
show bgp any-vrf ipv6 community no-export
show bgp ipv6 community
show bgp ipv6 community <*number*>
show bgp ipv6 community exact
show bgp ipv6 community internet
show bgp ipv6 community local-as
show bgp ipv6 community no-advertise
show bgp ipv6 community no-export
show bgp vrf <*name*> **ipv6 community**
show bgp vrf <*name*> **ipv6 community** <*number*>
show bgp vrf <*name*> **ipv6 community exact**
show bgp vrf <*name*> **ipv6 community internet**

show bgp vrf <*name*> **ipv6 community local-as**
show bgp vrf <*name*> **ipv6 community no-advertise**
show bgp vrf <*name*> **ipv6 community no-export**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

any-vrf	Optional. Displays BGP information for all virtual routing and forwarding (VRF) instances.
ipv4	Displays IPv4 BGP route information.
ipv6	Displays IPv6 BGP route information.
vrf <*name*>	Optional. Displays BGP information for a specific VRF instance.
<*number*>	Optional. Displays routes that contain this value in their community attribute. This is a numeric value that can be an integer from **1** to **4294967295** or string in the form ***aa:nn***, where the value of ***aa*** is the autonomous system (AS) number and the value of ***nn*** is the desired local preference to be used in the service provider network. Multiple community-number parameters can be present in the command.
exact	Optional. Displays only BGP routes that have the same communities.
internet	Optional. Displays routes that contain this value in their community attribute. This represents the well-known reserved community INTERNET.
local-as	Optional. Displays routes that contain this value in their community attribute. This represents the well-known reserved community string NO_EXPORT_SUBCONFED. Routes containing this attribute should not be advertised to external BGP peers.
no-advertise	Optional. Displays routes containing this value in the community attribute. This represents the well-known reserved community string NO_ADVERTISE. Routes containing this attribute should not be advertised to any BGP peer.
no-export	Optional. Displays routes containing this value in the community attribute. This represents the well-known reserved community string NO_EXPORT. Routes containing this attribute should not be advertised to BGP peers outside a confederation boundary.

Default Values

By default, this command displays all BGP routes.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products. Command was also expanded to include the **any-vrf**, **ipv4**, **vrf** <*name*>, and **exact** parameters.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products. Command was also expanded to include the **ipv6** parameter.

Usage Examples

In the following example, all BGP routes are displayed whose community numbers match those listed in the **show bgp community** command.

```
>enable
#show bgp ipv4 community local-as 10:405
BGP local router ID is 10.22.131.241, local AS is 302.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Path
10.22.152.20/30	10.22.131.10	304		302 300 1 3 4 i
10.22.152.24/29	10.22.131.10	304		302 300 1 3 4 5 i
10.22.152.36/30	10.22.131.10	304		302 300 1 3 4 i
10.22.152.52/30	10.22.131.10	304		302 300 1 3 4 i
11.0.0.0/30	10.22.131.10	304		302 300 1 3 4 6 i
12.0.0.0/30	10.22.131.10	304		302 300 1 3 4 6 i
13.0.0.0/30	10.22.131.10	304		302 300 1 3 4 6 i
14.0.0.0/30	10.22.131.10	304		302 300 1 3 4 6 i

```
Total RIB entries = 8
```

Information displayed includes: the ID of this router and its autonomous system (AS) number; the destination Network address of the route learned; the Next-Hop address to that network; the Metric; the Local Preference (LocPrf) value (set using the command **set local-preference**); and the AS Path to the destination network.

The following is sample output for the **show bgp ipv4 community** command with an exact match specified. BGP routes with the community numbers specified and *only* those specified are shown.

>**enable**
#show bgp ipv4 community 1001 2001 3001 exact
BGP local router ID is 192.168.9.1, local AS is 252.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	NextHop	Metric	LocPrf	Path
* 192.168.11.0/24	10.22.27.251	249	251	i
* 192.168.12.0/24	10.22.27.251	249	251	i
*> 192.168.32.0/24	10.22.27.249	249		i
*> 192.168.33.0/24	10.22.27.249	249		i

Total RIB entries = 4

show bgp community-list

Use the **show bgp community-list** command to display Border Gateway Protocol (BGP) routes that are permitted by the specified community list. Variations of this command include:

show bgp any-vrf ipv4 community-list *<list name>*
show bgp any-vrf ipv4 community-list *<list name>* **exact**
show bgp ipv4 community-list *<list name>*
show bgp ipv4 community-list *<list name>* **exact**
show bgp vrf *<name>* **ipv4 community-list** *<list name>*
show bgp vrf *<name>* **ipv4 community-list** *<list name>* **exact**
show bgp any-vrf ipv6 community-list *<list name>*
show bgp any-vrf ipv6 community-list *<list name>* **exact**
show bgp ipv6 community-list *<list name>*
show bgp ipv6 community-list *<list name>* **exact**
show bgp vrf *<name>* **ipv6 community-list** *<list name>*
show bgp vrf *<name>* **ipv6 community-list** *<list name>* **exact**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

any-vrf	Optional. Displays BGP information for all virtual routing and forwarding (VRF) instances.
ipv4	Displays IPv4 BGP route information.
ipv6	Displays IPv6 BGP route information.
vrf *<name>*	Optional. Displays BGP information for a specific VRF instance.
<list name>	Specifies the name of the community list whose routes you wish to display.
exact	Optional. Restricts the routes displayed to only those whose community lists exactly match those specified in the named community list. If this parameter is omitted, all routes matching any part of the specified community list will be displayed.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products. The command was also expanded to include the **any-vrf**, **ipv4**, and **vrf** <*name*> parameters.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products. The command was also expanded to include the **ipv6** parameter.

Functional Notes

Information displayed includes the ID of this router and its autonomous system (AS) number, the destination Network address of the route learned, the Next-Hop address to that network, the Metric, the Local Preference (LocPrf) value (set using the command **set local-preference *** on ????), and the AS Path to the destination network.

Usage Examples

In the following example, all IPv4 BGP routes are displayed whose community numbers match those defined in the community list named CList1.

```
>enable
#show bgp ipv4 community-list CList1
BGP local router ID is 10.22.131.241, local AS is 302.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network          Next Hop         Metric     LocPrf     Path
     10.22.152.20/30  10.22.131.10     304                   302 300 1 3 4 i
     10.22.152.24/29  10.22.131.10     304                   302 300 1 3 4 5 i
     10.22.152.36/30  10.22.131.10     304                   302 300 1 3 4 i
     10.22.152.52/30  10.22.131.10     304                   302 300 1 3 4 i
     11.0.0.0/30      10.22.131.10     304                   302 300 1 3 4 6 i
     12.0.0.0/30      10.22.131.10     304                   302 300 1 3 4 6 i
     13.0.0.0/30      10.22.131.10     304                   302 300 1 3 4 6 i
     14.0.0.0/30      10.22.131.10     304                   302 300 1 3 4 6 i
     20.0.0.0/30      10.22.131.10     304                   302 300 1 3 4 5 i
     21.0.0.0/30      10.22.131.10     304                   302 300 1 3 4 5 i
Total RIB entries = 10
```


show bgp neighbors

Use the **show bgp neighbors** command to display information for the specified Border Gateway Protocol (BGP) neighbor. Variations of this command include the following:

show bgp any-vrf ipv4 neighbors
show bgp any-vrf ipv4 neighbors <*ipv4 address*>
show bgp any-vrf ipv4 neighbors <*ipv4 address*> **advertised-routes**
show bgp any-vrf ipv4 neighbors <*ipv4 address*> **received-routes**
show bgp any-vrf ipv4 neighbors <*ipv4 address*> **routes**
show bgp any-vrf ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show bgp any-vrf ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] advertised-routes**
show bgp any-vrf ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] received-routes**
show bgp any-vrf ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] routes**
show bgp ipv4 neighbors
show bgp ipv4 neighbors <*ipv4 address*>
show bgp ipv4 neighbors <*ipv4 address*> **advertised-routes**
show bgp ipv4 neighbors <*ipv4 address*> **received-routes**
show bgp ipv4 neighbors <*ipv4 address*> **routes**
show bgp ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show bgp ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] advertised-routes**
show bgp ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] received-routes**
show bgp ipv4 neighbors <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] routes**
show bgp vrf <*name*> **ipv4 neighbors**
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*>
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*> **advertised-routes**
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*> **received-routes**
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*> **routes**
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] advertised-routes**
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] received-routes**
show bgp vrf <*name*> **ipv4 neighbors** <*ipv4 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] routes**
show bgp any-vrf ipv6 neighbors
show bgp any-vrf ipv6 neighbors <*ipv6 address*>
show bgp any-vrf ipv6 neighbors <*ipv6 address*> **advertised-routes**

show bgp any-vrf ipv6 neighbors <*ipv6 address*> **received-routes**
show bgp any-vrf ipv6 neighbors <*ipv6 address*> **routes**
show bgp any-vrf ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show bgp any-vrf ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] advertised-routes**
show bgp any-vrf ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] received-routes**
show bgp any-vrf ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] routes**
show bgp ipv6 neighbors
show bgp ipv6 neighbors <*ipv6 address*>
show bgp ipv6 neighbors <*ipv6 address*> **advertised-routes**
show bgp ipv6 neighbors <*ipv6 address*> **received-routes**
show bgp ipv6 neighbors <*ipv6 address*> **routes**
show bgp ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show bgp ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] advertised-routes**
show bgp ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] received-routes**
show bgp ipv6 neighbors <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] routes**
show bgp vrf <*name*> **ipv6 neighbors**
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*>
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*> **advertised-routes**
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*> **received-routes**
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*> **routes**
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] advertised-routes**
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] received-routes**
show bgp vrf <*name*> **ipv6 neighbors** <*ipv6 address*> **[mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] routes**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

any-vrf	Optional. Displays BGP information for all virtual routing and forwarding (VRF) instances.
ipv4	Displays IPv4 BGP route information.
ipv6	Displays IPv6 BGP route information.
vrf <*name*>	Optional. Displays BGP information for a specific VRF instance.
<*ipv4 address*>	Optional. Displays information for the specified neighbor. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
	If no IPv4 address is entered, information for all neighbors is displayed.
<*ipv6 address*>	Optional. Displays information for the specified neighbor. IPv6 addresses should be expressed in colon hexadecimal format (for example, **2001:DB8:1::1**).
	If no IPv6 address is entered, information for all neighbors is displayed.
advertised-routes	Optional. Displays all routes being advertised to the specified neighbor. Command output is the same as for **show bgp** except filtered to only the BGP routes being advertised to the specified neighbor.
received-routes	Optional. Displays all routes (accepted and rejected) advertised by the specified neighbor. Routes may be rejected by inbound filters, such as prefix list filters.
routes	Optional. Displays all accepted received routes advertised by the specified neighbor. Routes displayed have passed inbound filtering. This command output is the same as **show ip bgp** except the output is filtered to those learned from the specified neighbor.
mef-ethernet <*slot/port*>	Optional. Displays information for the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Displays information for neighbors in the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Displays information for neighbors in the system management EVC.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products. Command was also expanded to include the **any-vrf**, **ipv4**, and **vrf** <*name*> parameters.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products. Command was also expanded to include the **ipv6** and <*ipv6 address*> parameters.

Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

Entries that are not filtered by prefix lists are marked with an asterisk (*) to show they are valid. Entries that are deemed the best path to advertised route are marked with a caret (>).

Usage Examples

The following are output variations of the **show bgp ipv4 neighbors** command:

```
>enable
#show bgp ipv4 neighbors
BGP neighbor is 10.15.43.17, remote AS 100, external link
Configured hold time is 180, keepalive interval is 60 seconds
Default minimum time between advertisement runs is 30 seconds
Connections established 6; dropped 5
Last reset: Interface went down
 Connection ID: 15
   BGP version 4, remote router ID 8.1.1.1
   BGP state is Established, for 01:55:05
   Negotiated hold time is 180, keepalive interval is 60 seconds
   Message statistics:
    InQ depth is 0, OutQ depth is 0
Local host: 10.15.43.18, Local port: 179
         Sent     Rcvd
    Opens:1      1
    Notifications: 00
    Updates: 0   8
    Keepalives: 116116
    Unknown: 0 0
    Total: 117     125
Foreign host: 10.15.43.17, foreign port: 1048
   Flags: passive open

#show bgp ipv4 neighbors 10.15.43.34 advertised-routes
BGP local router ID is 10.0.0.1, local AS is 101.
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          NextHop          Metric Path
*>    1.0.0.0/8        10.15.43.17      1 100 i
*>    2.0.0.0/9        10.15.43.17      1 100 i
```


#show bgp ipv4 neighbors 10.15.43.17 received-routes

BGP local router ID is 10.0.0.1, local AS is 101.
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	NextHop	Metric Path
*>	1.0.0.0/8	10.15.43.17	1 100 i
*>	2.0.0.0/9	10.15.43.17	1 100 i

#show ip bgp neighbors 10.15.43.17 routes

BGP local router ID is 10.0.0.1, local AS is 101.
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	NextHop	Metric Path
*>	1.0.0.0/8	10.15.43.17	1 100 i
*>	2.0.0.0/9	10.15.43.17	1 100

show bgp regexp <*expression*>

Use the **show bgp regexp** command to display a summary of the Border Gateway Protocol (BGP) route table that includes routes whose autonomous system (AS) path matches the specified expression. Variations of this command include:

show bgp any-vrf ipv4 regexp <*expression*>
show bgp ipv4 regexp <*expression*>
show bgp vrf <*name*> **ipv4 regexp** <*expression*>
show bgp any-vrf ipv6 regexp <*expression*>
show bgp ipv6 regexp <*expression*>
show bgp vrf <*name*> **ipv6 regexp** <*expression*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*expression*>	Displays routes whose AS path matches the regular expression specified.
any-vrf	Optional. Displays BGP information for all virtual routing and forwarding (VRF) instances.
ipv4	Displays IPv4 BGP route information.
ipv6	Displays IPv6 BGP route information.
vrf <*name*>	Optional. Displays BGP information for a specific VRF instance.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products. Command was also expanded to include the **any-vrf**, **ipv4**, and **vrf** <*name*> parameters.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products. Command was also expanded to include the **ipv6** parameter.

Functional Notes

Entries that are not filtered by prefix lists are marked with an asterisk (*) to show they are valid. Entries that are deemed the best path to advertised route are marked with a caret (>).

Usage Examples

The following sample output of the **show bgp ipv4 regexp _303_** command shows all of the entries in the BGP database that contain “303” in the AS path.

```
>enable
#show bgp ipv4 regexp _303_
BGP local router ID is 192.168.3.1, local AS is 304.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete
Network              NextHop Metric      LocPrf Path
10.22.130.8/29       10.22.132.9          303 304 302 i
* i10.22.130.240/28  0.22.132.1           100 303 300 i
* 10.22.130.240/28   10.22.132.9          303 300 i
10.22.131.0/29       10.22.132.9          303 304 302 i
10.22.131.8/29       10.22.132.9          303 304 302 i
* i10.22.131.16/29   10.22.132.1          0 100 303 i
* 10.22.131.16/29    10.22.132.9          0 303 i
* i10.22.131.240/28  10.22.132.1          100 303 300 i
* 10.22.131.240/28   10.22.132.9          303 300 i
* 10.22.132.0/29     10.22.131.1          0 302 303 i
* 10.22.132.0/29     10.22.131.9          0 302 303 i
* i10.22.132.0/29    10.22.132.1          0 100 303 i
*> 10.22.132.0/29    10.22.132.9          0 303 i
* 10.22.132.8/29     10.22.131.1          0 302 303 i
* 10.22.132.8/29     10.22.131.9          0 302 303 i
* 10.22.132.8/29     10.22.132.9          0 303 i
* i10.22.132.240/28  10.22.132.1          0 100 303 i
*> 10.22.132.240/28  10.22.132.9          0 303 i
10.22.134.0/29       10.22.132.9          303 304 i
10.22.134.8/29       10.22.132.9          303 304 i
10.22.134.16/29      10.22.132.9          303 304 i
10.22.134.24/29      10.22.132.9          303 304 i
10.22.134.32/29      10.22.132.9          303 304 i
10.22.134.40/29      10.22.132.9          303 304 i
10.22.134.48/29      10.22.132.9          303 304 i
10.22.134.56/29      10.22.132.9          303 304 i
10.22.134.64/29      10.22.132.9          303 304 i
10.22.134.80/29      10.22.132.9          303 304 i
10.22.135.0/29       10.22.132.9          303 304 305 i
10.22.135.8/29       10.22.132.9          303 304 305 i
Total RIB entries = 30
```

show bridge

Use the **show bridge** command to display a list of all configured bridge groups (including individual members of each group). Enter an interface or a bridge number to display the corresponding list. Variations of this command include:

show bridge
show bridge <*interface*>
show bridge <*number*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*interface*>	Optional. Displays all bridge groups associated with the specific interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type the **show bridge ?** command to display a list of applicable interfaces.
<*number*>	Optional. Displays a specific bridge group.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) interface.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following is sample output from the **show bridge** command:

>**enable**
#show bridge
Total of 300 station blocks 295 free

Address	Action	Interface	Age	Rx Count	Tx Count
00:04:51:57:4D:5A	forward	eth 0/1	0	7133392	7042770
00:04:5A:57:4F:2A	forward	eth 0/1	0	402365	311642
00:10:A4:B3:A2:72	forward	eth 0/1	4	2	0
00:A0:C8:00:8F:98	forward	eth 0/1	0	412367	231
00:E0:81:10:FF:CE	forward	fr 1.17	0	1502106	1486963

show buffers

Use the **show buffers** command to display the statistics for the buffer pools on the network server. Variations of this command include:

show buffers
show buffers realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

The **show buffers** command is not available on vAOS instances.

Usage Examples

The following is sample output from the **show buffers** command:

>**enable**
#show buffers
Buffer handles: 119 of 2000 used.

Pool	Size	Total	Used	Available	Max. Used
0	1800	1894	119	1775	122
1	2048	64	0	64	0
2	4096	32	0	32	0
3	8192	4	0	4	0

show buffers users

Use the **show buffers users** command to display a list of the top users of packet buffers. Typically, this command will only be used as a debug tool by Adtran personnel. Variations of this command include:

show buffers users
show buffers users realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

The **show buffers users** command is not available for vAOS instances.

Usage Examples

The following is sample output from the **show buffers users** command:

>**enable**
#show buffers users
Number of users: 7

Ran	User	Count
1	0x0052f4f8	59
2	0x0051a4fc	32
3	0x00528564	8
4	0x0053c1c8	7
5	fixedsize	5
6	0x001d8298	2
7	0x0010d970	1
8	0x00000000	0
9	0x00000000	0
10	0x00000000	0
11	0x00000000	0

show cflash

Use the **show cflash** command to display a list of all files currently stored in CompactFlash® memory or details about a specific file stored in CompactFlash memory. Variations of this command include:

show cflash
show cflash *<filename>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<filename>	Optional. Displays details for a specified file located in flash memory. Enter a wildcard (such as ***.biz**) to display the details for all files matching the entered pattern.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show cflash** command:

```
>enable
#show cflash
(dir)      0 SystemDefaultPrompts
(dir)      0 VoiceMail
9377163 NV7100A-12-00-23-E.biz
11110890 sip.ld
8767439 NV7100A-11-03-02-E.biz
8771176 NV7100A-11-03-02d-E.biz
8773148 NV7100A-11-03-03-E.biz
48508928 bytes used, 207319040 available, 255827968 total
```


show channel-group

Use the **show channel-group** command to display detailed information regarding port aggregation of a specified channel group (i.e., channel groups and their associated ports). Variations of this command include the following:

show channel-group port-channel load-balance
show channel-group summary
show channel-group <*number*> **summary**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

port-channel load-balance	Displays the current load-balance scheme.
summary	Summarizes the state of all channel groups or of a specific channel group (if specified by the <*number*> argument).
<*number*>	Optional. Specifies the channel group using the channel group ID (16).

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show channel-group** command:

```
>enable
#show channel-group summary
Channel Group        Port channel        Associated Ports
---------------------  -----------------  ------------------------
1                    1                  eth 0/2 eth 0/3
2                    2                  eth 0/5 eth 0/6 eth 0/7
```


show clock

Use the **show clock** command to display the system time and date entered using the **clock set** command. Refer to *clock set <time> <day> <month> <year> on page 223* for more information. Variations of this command include:

show clock
show clock detail

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Optional. Displays more detailed clock information, including the time source.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays the current time and data from the system clock:

```
>enable
#show clock
23:35:07 UTC Tue Aug 20 2002
```


show cloudinit output-errors

Use the **show cloudinit output-errors** command to display any errors that occurred during the boot process of a virtual AOS (vAOS) instance.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R12.2.0	Command was introduced.

Functional Notes

vAOS has the ability to read special configuration files that are present in a virtual environment, and take them into consideration when making decisions about its initial configuration. If any errors occur during this process, they can be displayed using the **show cloudinit output-errors** command.

Usage Examples

The following example displays any errors that occurred in the vAOS boot process:

```
>enable
#show cloudinit output-errors
```


show command-mode

Use the **show command-mode** command to display the command mode in AOS for a specific set of configuration commands. There are multiple levels of access within AOS from which users are allowed to execute configuration commands. This command is used to verify the mode to which access must be granted to execute a specific set of commands. This command is used for setting privilege levels for users to access the AOS CLI. Variations of this command include:

do show command-mode
show command-mode

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

do	Specifies executing an Enable mode command from within the active configuration mode. Any **show** command can be entered from any configuration mode as long as it is preceded by the **do** command.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

Since this command can be entered from anywhere in AOS, it has two variations. The **show command-mode** command can only be issued from within the Enable Configuration mode. The **do show command-mode** can only be entered from a configuration mode such as Global, or an interface configuration mode. The command mode is necessary information for setting specific privilege levels in AOS. For more information about privilege levels, refer to the command *privilege <mode> level <level> on page 1663* of this guide and the configuration guide *Configuring Privilege Levels in AOS CLI* available online at http://supportforums.adtran.com.

Usage Examples

The following example displays the current command mode from within the Enable mode where all **show** and **debug** commands are entered:

>**enable**
#show command-mode
Command mode is 'exec'

The following example displays the current command mode from within the Global Configuration mode where a majority of the configuration commands are entered that affect the AOS device on a global level:

>**enable**
#configuration terminal
(config)**#do show command-mode**
Command mode is 'config'

show community-list

Use the **show community-list** command to display any or all defined community lists in the router configuration. Variations of this command include:

show community-list
show community-list *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Optional. Specifies the name of the community list you wish to display. If this parameter is omitted, all defined community lists will be displayed.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran products.

Usage Examples

The following example shows two community lists, one of which permits all routes containing community number 10:67, and another which permits routes containing community number 10:68 and the Internet community number, but denies routes containing community number 10:45.

```
>enable
#show community-list
community-list CommList1:
 permit 10:67
community-list CommList2:
 permit 10:68 internet
 deny 10:45
```


show configuration

Use the **show configuration** command to display a text printout of the startup configuration file stored in nonvolatile random access memory (NVRAM).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show configuration** command:

```
>enable
#show configuration
!
!
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
logging forwarding priority-level info
no logging email
!
ip policy-timeout tcp all-ports 600
ip policy-timeout udp all-ports 60
ip policy-timeout icmp 60
```



```
!
!
!
interface eth 0/1
speed auto
 no ip address
 shutdown
!
interface dds 1/1
 shutdown
!
interface bri 1/2
 shutdown
!
!
ip access-list standard Outbound
 permit host 10.3.50.6
 permit 10.200.5.0 0.0.0.255
!
!
ip access-list extended UnTrusted
 deny   icmp 10.5.60.0 0.0.0.255 any source-quench
 deny   tcp any any
!
no snmp agent
!
!
!
line con 0
 no login
!
line telnet 0
 login
line telnet 1
 login
line telnet 2
 login
line telnet 3
 login
line telnet 4
 login
!
```


show connections

Use the **show connections** command to display information (including time division multiplexing (TDM) group assignments) for all active connections.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show connections** command:

```
>enable
#show connections
Displaying all connections....
```

Conn ID	From	To
1	atm 1	adsl 1/1
2	ppp 1	t1 2/1, tdm-group 1
3	ppp 1	t1 2/2, tdm-group 1
4	ppp 3	e1 3/1, tdm-group 1
5	ppp 3	e1 3/2, tdm-group 1
6	ppp 3	e1 3/3, tdm-group 1

show crypto ca

Use the **show crypto ca** command to display information regarding certificates and profiles. Variations of this command include:

show crypto ca certificates
show crypto ca crls
show crypto ca profiles

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

certificates	Displays information on all certificates.
crls	Displays a summary of all certificate revocation lists (CRLs) for each certificate authority (CA).
profiles	Displays information on all configured CA profiles.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced (enhanced software version only).
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show crypto ca certificates** command:

```
>enable
#show crypto ca certificates
CA Certificate
 Status: Available
 Certificate Serial Number: 012d
 Subject Name: /C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1
 Issuer: /C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1
 CRL Dist. Pt: /C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1
 Start date is Jan 9 16:25:15 2003 GMT
 End date is Dec 31 23:59:59 2003 GMT
 Key Usage:
   Non-Repudiation
   Key Encipherment
   Data Encipherment
   CRL Signature
   Encipherment Only
```

show crypto ike

Use the **show crypto ike** command to display information regarding the Internet key exchange (IKE) configuration. Variations of this command include the following:

show crypto ike client configuration pool
show crypto ike client configuration pool *<name>*
show crypto ike policy
show crypto ike policy *<value>*
show crypto ike remote-id *<remote-id>*
show crypto ike sa
show crypto ike sa brief

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

client configuration pool	Displays the list of all configured IKE client configuration pools.
<name>	Optional. Displays detailed information regarding the specified IKE client configuration pool.
policy	Displays information on all IKE policies. Indicates if client configuration is enabled for the IKE policies and displays the pool names.
<value>	Optional. Displays detailed information on the specified IKE policy. This number is assigned using the **crypto ike policy** command. Refer to *crypto ike on page 1247* for more information.
remote-id *<remote-id>*	Displays information on all IKE information regarding the remote-id. The remote-id value is specified using the **crypto ike remote-id** command. Refer to *crypto ike remote-id on page 1251* for more information.
sa	Displays all Internet Protocol security (IPsec) security associations (SAs).
sa brief	Optional. Displays a brief listing of IPsec SAs.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 15.1	Command was expanded to include the **brief** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show crypto ike policy** command:

```
>enable
#show crypto ike policy
Crypto IKE Policy 100
 Main mode
 Using System Local ID Address
 Peers:
  63.105.15.129
initiate main
respond anymode
 Attributes:
    10
      Encryption: 3DES
      Hash: SHA
      Authentication: Pre-share
      Group: 1
      Lifetime: 900 seconds
```

The following is sample output from the **show crypto ike sa brief** command:

```
>enable
#show crypto ike sa brief
Using 3 SAs out of 2000
IKE Security Associations:

(NOTE: The Remote ID may be truncated)

Peer IP Address  Lifetime  Status           IKE Policy  Remote ID
10.22.19.4       19800     UP (SA_MATURE)   100         nv1224r
10.22.19.2       0         MM_SA_WAIT       101         UNKNOWN
10.22.19.6       86365     UP (SA_MATURE)   102         security2
```

show debugging

Use the **show debugging** command to display a list of all activated debug message categories. Variations of this command include:

show debugging
show debugging saved-filters

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

saved-filters	Optional. Displays the last debug filters saved using the command *debug save on page 450*.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.4	Command was expanded to include the **saved-filters** keyword.

Usage Examples

The following is sample output from the **show debugging** command:

```
>enable
#show debugging
debug ip access-list MatchAll
debug firewall
debug ip rip
debug frame-relay events
debug frame-relay llc2
debug frame-relay lmi
```


The following is sample output from the **show debugging saved-filters** command:

>**enable**
#show debugging saved-filters
Saved filters:
debug mail-client agent
debug probe test1

show demand

Use the **show demand** command to display information regarding demand routing parameters and statistics. Variations of this command include the following:

show demand
show demand interface demand <*interface*>
show demand resource pool
show demand resource pool <*name*>
show demand sessions

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interface demand <*interface*>	Optional. Displays information for a specific demand routing interface. Valid range is **1** to **1024**. Type **show demand interface ?** for a list of valid interfaces.
resource pool	Optional. Displays all resource pool information.
<*name*>	Optional. Displays resource pool information for a specific resource pool name.
sessions	Optional. Displays active demand sessions.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show demand interface** command:

```
>enable
#show demand int 1
Demand 1 is UP (connected)
 Configuration:
   Keep-alive is set (10 sec.)
   Admin MTU = 1500
```



```
   Mode: Either, 1 dial entries, idleTime = 120, fastIdle = 20
   Resource pool demand
   No authentication configured
   IP address 10.100.0.2 255.255.255.0
 Connect Sequence: Successes = 0, Failures = 0
   Seq    DialString     Technology    Successes  Busys   NoAnswers    NoAuths    InUse
    5      5552222          ISDN            0        0          0           0
 Current values:
   Local IP address 10.100.0.2, Peer IP address 10.100.0.1
   Seconds until disconnect: 63
   Queueing method: weighted fair
   Output queue: 0/1/428/64/0 (size/highest/max total/threshold/drops)
     Conversations 0/1/256 (active/max active/max total)
     Available Bandwidth 48 kilobits/sec
   Bandwidth=64 Kbps
 Link through bri 1/3, Uptime 0:01:10
   IN: Octets 588, Frames 19, Errors 0
   OUT: Octets 498, Frames 18, Errors 0
   Last callerID 2565552222, last called num 5552222
```

The following is sample output from the **show demand interface demand** command:

```
>enable
#show demand interface demand 1
demand 1
Idle timer (120 secs), Fast idle timer (20 secs)

Dialer state is data link layer up
Dial reason: answered

Interface bound to resource bri 1/3
Time until disconnect 105 secs
Current call connected 00:00:27
Connected to 2565552222

Number of active calls = 1
Interesting Traffic = list junk

 Connect Sequence: Successes = 0, Failures = 0
   Seq    DialString     Technology    Successes     Busys  NoAnswers    NoAuths    InUse
    5      5552222         ISDN0            0          0          0
```


The following is sample output from the **show demand resource pool** command:

```
>enable
#show demand resource pool
Pool demand
        Resources:          bri 1/3, bri 2/3
        Demand Interfaces:  demand 1
```

The following is sample output from the **show demand sessions** command:

```
>enable
#show demand sessions
Session 1
Interface demand 1
Local IP address = 10.100.0.2
Remote IP address = 10.100.0.1
Remote Username =
Dial reason: ip (s=, d=)
Link 1
 Dialed number = 5552222
 Resource interface = bri 1/3, Multilink not negotiated
 Connect time: 0:0:13
 Idle Timer: 119
```


show desktop-auditing dhcp

Use the **show desktop-auditing dhcp** command to display collected network access protection (NAP) and Dynamic Host Configuration Protocol (DHCP) information for clients connected to the network. The display of the collected information can be for all connected clients or for a specific client. Variations of this command include:

show desktop-auditing dhcp
show desktop-auditing dhcp antispyware 3rd-party
show desktop-auditing dhcp antispyware disabled
show desktop-auditing dhcp antispyware out-of-date
show desktop-auditing dhcp antispyware snoozed
show desktop-auditing dhcp antivirus 3rd-party
show desktop-auditing dhcp antivirus disabled
show desktop-auditing dhcp antivirus out-of-date
show desktop-auditing dhcp antivirus snoozed
show desktop-auditing dhcp auto-updates disabled
show desktop-auditing dhcp auto-updates not-checking
show desktop-auditing dhcp auto-updates not-downloading
show desktop-auditing dhcp auto-updates not-installing
show desktop-auditing dhcp brief
show desktop-auditing dhcp firewall 3rd-party
show desktop-auditing dhcp firewall disabled
show desktop-auditing dhcp firewall snoozed
show desktop-auditing dhcp hostname <*hostname*>
show desktop-auditing dhcp interface gigabit-switchport <*slot/port*>
show desktop-auditing dhcp ip <*ip address*>
show desktop-auditing dhcp local-violators
show desktop-auditing dhcp mac <*mac address*>
show desktop-auditing dhcp server-restricted
show desktop-auditing dhcp server-violators

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

antispyware	Optional. Displays NAP information only for clients with the specified antispyware status.
3rd-party	Displays NAP information only for clients with third-party antispyware.

disabled	Displays NAP information only for clients with disabled antispyware.
out-of-date	Displays NAP information only for clients with out-of-date antispyware.
snoozed	Displays NAP information only for clients with inactive antispyware.
antivirus	Optional. Displays NAP information only for clients with the specified antivirus status.
3rd-party	Displays NAP information only for clients with third-party antivirus software.
disabled	Displays NAP information only for clients with disabled antivirus software.
out-of-date	Displays NAP information only for clients with out-of-date antivirus software.
snoozed	Displays NAP information only for clients with inactive antivirus software.
auto-updates	Optional. Displays NAP information only for clients with the specified auto-update status.
disabled	Displays NAP information only for clients with disabled auto-updates.
not-checking	Displays NAP information only for clients that are not checking for auto-updates.
not-downloading	Displays NAP information only for clients that are not downloading auto-updates.
not-installing	Displays NAP information only for clients that are not installing auto-updates.
brief	Optional. Displays information for all NAP clients in a table format.
firewall	Optional. Displays NAP information only for clients with the specified firewall state.
3rd-party	Displays NAP information only for clients with third-party firewall software.
disabled	Displays NAP information only for clients with disabled firewall software.
snoozed	Displays NAP information only for clients with inactive firewall software is displayed.
hostname <*hostname*>	Optional. Displays NAP information only for the client with the specified host name.
interface gigabit-switchport <*slot/port*>	Optional. Displays NAP information only for the client using the specified interface.
ip <*ip address*>	Optional. Displays NAP information only for the client at the specified IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

local-violators	Optional. Displays NAP information only for clients that violate the local policy.
mac <*mac address*>	Optional. Displays NAP information only for the client at the specified medium access control (MAC) address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
server-restricted	Optional. Displays NAP information only for the clients restricted by the server.
server-violators	Optional. Displays NAP information only for the clients that violate the server policy.

Default Values

No default values are necessary for this command.

Command History

Release 17.8	Command was introduced.

Functional Notes

Output of the **show desktop-auditing dhcp** command can be limited by specific client or by specific criteria (feature states), but not by both.

Local policies are defined by using the command *desktop-auditing local-policy on page 1258*.

For more information about configuring local policies, refer to *Desktop Auditing Local Policy Command Set on page 4395*.

For more information about configuring desktop auditing, refer to the *Configuring Desktop Auditing in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following is sample output from the **show desktop-auditing dhcp** command:

```
#show desktop-auditing dhcp
Client MAC/IP: 00:E0:29:0E:D5:E3 / 10.23.220.1 / xpsp3-host
    Collected: DHCP
    VLAN ID: 100
    Source Port: gigabit-switchport 0/2
    Date/Time Collected: 2009.08.25 10:33:42
    Client NAP: Enabled
    Server NAP: Enabled
    Client OS Version: Windows XP
    Client OS Service Pack: 3
    Client Processor Architecture: x86 architecture
    Client Firewall:  Microsoft
                      Disabled but Up-To-Date
    Client Antivirus: Symantec Antivirus Corporate Edition
```



```
                    Enabled & Up-To-Date
  Client Antispyware: None Installed
  Client Automatic Security Updates: Enabled, Download, but Don't Install
  Client Security Updates: From 10.10.10.3
                           Up-To-Date (2009.08.25 10:33:42)
  Client Requires Remediation: False
  Network Connectivity: Not restricted
```

The preceding output is for one client. This same information will be displayed for all connected clients unless one of the filtering parameters is used in conjunction with the ***show desktop-auditing dhcp*** *command.*

The following is sample output from the **show desktop-auditing dhcp brief** command. Because of the **brief** keyword, the results are displayed in table format.

#show desktop-auditing dhcp brief

```
Columns:          E = Enabled, U = Up-to-date, 3 = 3rd party (not MS), S = Snoozed
                  C = Check for Updates, D = Download Updates, I = Install Updates
                  ! = Error (not installed, other)
Indicators:       + = True, - = False, ? = Unknown State
                  ! = Attention
Server
Response          R = Client Requires Remediation, N = Client Network Restricted
Codes:            . = No Server Response

Client              FireWall    AntiVir     AntiSpy     AutoUpd     SecUpd      Server
                      E3S!       EU3S!       EU3S!       ECDI!      Severity    Response
    ------------------------------------------------------------------------------------------------------------------------
00:E0:29:0E:D5:E3     +--         +++-        +++-        ++--       Important
00:E0:29:0E:D5:E4     ---         +-+-        ----!       ++++       Low         RN
```


show dial-backup interfaces

Use the **show dial-backup interfaces** command to display all configured dial-backup interfaces and the associated parameters for each.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) dial backup.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example enters the Enable mode and uses the show command to display dial-backup interface information:

```
>enable
#show dial-backup interfaces
Dial-backup interfaces...
fr 1.16 backup interface:
 Backup state: idle
 Backup protocol: PPP
Call mode: originate
 Auto-backup: enabled
 Auto-restore: enabled
 Priority: 50
 Backup delay: 10 seconds
 Restore delay: 10 seconds
 Connect timeout: 60 seconds
--MORE--
```


show dialin interfaces

Use the **show dialin interfaces** command to display information regarding remote console dialin.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show dialin interfaces** command:

```
>enable
#show dialin interfaces
Dialin interfaces...
modem 1/3 dialin interface:
 Connection Status: Connected
Caller ID info: name-John Smith number-5551212 time-14:23:10 2/17/2003
```


show dos counters

Use the **show dos counters** command to display denial of service (DoS) attack statistics.

Syntax Description

No subcommands.

Default Values

By default, DoS protection in AOS is disabled.

Command History

Release 17.7	Command was introduced.

Usage Examples

The following example displays attack statistics for the AOS unit:

```
>enable
#show dos counters
DOS Fragment Error 0
DOS ICMP Error 0
DOS L3 Header Error 0
DOS L4 Header Error 1269620
DOS Source MAC equal Destination MAC  0
#
```

show dos-id

Use the **show dos-id** command to list all denial of service (DoS) attacks the DoS protection feature provides protection against, along with their corresponding threat IDs.

Syntax Description

No subcommands.

Default Values

By default, DoS protection in AOS is disabled.

Command History

Release 17.7	Command was introduced.

Functional Notes

The IDs obtained with the **show dos-id** command are used in the **dos-protection** <*id*> command to add or remove threat protection for specific threats.

Usage Examples

The following is sample output for this command:

```
>enable
#show dos-id
DOS L4 Header Error
  TCP pkts w/ control flags and seq# equal to 0                    [1]
  TCP pkts w/ SYN and FIN bits set                                 [2]
  TCP pkts w/ FIN,URG,PSH bits set with ACK bit & seq# equal to 0  [3]
  TCP pkts w/ source port equal to destination port                [4]
  UDP pkts w/ source port equal to destination port                [5]
  TCP SYN pkts w/source port 0-1023 for the first fragment         [6]

DOS L3 Header Error
  Source IP equal to Destination IP                                [20]

DOS ICMP Error
  Fragmented ICMP pkts                                             [40]
  ICMPV4 ping pkts w/payload greater than specified                [41]
  ICMPV6 ping pkts w/payload greater than specified                [42]

DOS Fragment Error
  TCP fragments w/ offset value set to 1                           [60]
  First TCP fragments w/ TCP header smaller than specified         [61]
#
```


show dot11 access-point

Use the **show dot11 access-point** command to display information about wireless access points (APs) for the wireless access controllers (ACs) in the network. Variations of this command include the following:

show dot11 access-point
show dot11 access-point detail
show dot11 access-point mac-address <*mac address*>
show dot11 access-point mac-address <*mac address*> **detail**
show dot11 access-point managed
show dot11 access-point managed detail
show dot11 access-point managed realtime
show dot11 access-point name <*name*>
show dot11 access-point name <*name*> **detail**
show dot11 access-point realtime
show dot11 access-point status available
show dot11 access-point status available detail
show dot11 access-point status download
show dot11 access-point status download detail
show dot11 access-point status init
show dot11 access-point status init detail
show dot11 access-point status no_session
show dot11 access-point status no_session detail
show dot11 access-point status ready
show dot11 access-point status ready detail
show dot11 access-point status recovery
show dot11 access-point status recovery detail
show dot11 access-point status running
show dot11 access-point status running detail
show dot11 access-point status session
show dot11 access-point status session detail
show dot11 access-point unmanaged
show dot11 access-point unmanaged detail
show dot11 access-point unmanaged realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

> NOTE *Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

mac-address <*mac address*>	Optional. Displays a particular access point (AP) by medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
managed	Optional. Displays a list of APs managed by this AC.
name <*name*>	Optional. Displays a particular AP by name.
status	Optional. Displays APs at a certain status. (Refer to the options below.)
available	Optional. Displays APs at available session state.
download	Optional. Displays APs at download state.
init	Optional. Displays APs at init state.
no_session	Optional. Displays APs at no session state.
ready	Optional. Displays APs at ready state.
recovery	Optional. Displays APs at recovery state.
running	Optional. Displays APs at running state.
session	Optional. Displays APs at session state.
unmanaged	Optional. Displays a list of APs not managed by this AC.
detail	Optional. Displays a detailed list of all discovered APs.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release 16.1	Command was expanded to include the available session state.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show dot11 access-point** command:

>**enable**
#show dot11 access-point
Wireless Access Points:

Name	MAC-Address	AP Status	Cfg'd	Control Status
ADTN1DF857	00:A0:C8:1D:F8:57	Session	Y	Ctl_by_This_AC

show dot11 clients

Use the **show dot11 clients** command to display stations associated with all wireless access points (APs). Variations of this command include the following:

show dot11 clients interface dot11ap *<ap interface>*
show dot11 clients mac-address *<mac address>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

interface dot11ap	Displays stations associated with APs by interface.
<ap interface>	Specifies AP interface number. Range is **1** to **8**.
mac-address	Displays stations associated with APs by medium access control (MAC) address.
<mac address>	Specifies a valid client 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following command initiates a request to display a list of clients for AP interface 1.

```
>enable
#show dot11 clients interface dot11ap 1
Wireless Access Point Clients:
 Ap        Station MAC-Address
 ------    -------------------
  1        00:40:96:AB:3B:5E
```


The following command initiates a request to display a list of clients for MAC address 00:40:96:ab:3b:5e:

>**enable**
#show dot11 clients mac-address 00:40:96:ab:3b:5e
Wireless Access Point Clients:

Ap	Radio	Vap	Station MAC-Address
1	1	1	00:40:96:AB:3B:5E

show dot11 statistics interface dot11ap

Use the **show dot11 statistics interface dot11ap** command to display counters of an 802.11 radio and its virtual access points (VAPs). Variations of this command include the following:

show dot11 statistics interface dot11ap *<ap/radio>*
show dot11 statistics interface dot11ap *<ap/radio.vap>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<ap>	Specifies the wireless access point (AP). Range is **1** to **8**.
</radio>	Specifies the radio associated with the AP. Range is **1** to **2**.
<.vap>	Specifies the VAP associated with the radio. Range is **1** to **8**.

> *The radio must be specified in the format <ap/radio>. For example, **2/1** indicates radio 1 on access point 2. The VAP must be specified in the format <ap/radio.vap>. For example, **2/1.1** indicates virtual access point 1 on radio 1 on access point 2.*

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output for the radio 1 on AP interface 1 using the **show dot11 statistics interface dot11ap** command:

```
>enable
#show dot11 statistics interface dot11ap 1/1
Authentication Count: 17
 Deauthentication Count: 48
 Association Count: 18
 Disassociation Count: 12
 Reassociation Count: 0
 Wireless MSDU Rx Packets: 346
 Wireless Data Rx Packets: 7221
 Wireless Multicast Rx Packets: 308
 Wireless Management Rx Packets: 675805
 Wireless Control Rx Packets: 0
 Wireless MSDU Tx Packets: 237259
 Wireless Data Tx Packets: 236856
 Wireless Multicast Tx Packets: 236812
 Wireless Management Tx Packets: 599
 Wireless Control Tx Packets: 0
```


show dns resolver queue

Use the **show dns resolver queue** command to show information related to the domain naming system (DNS) queries that are currently scheduled for resolution.Variations of this command include:

show dns resolver queue
show dns resolver queue realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release R11.6.0	Command was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C)**. If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following command shows real time information related to DNS queries currently scheduled for resolution:

>enable
#show dns resolver queue realtime

show dynamic-dns

Use the **show dynamic-dns** command to show information related to the dynamic domain naming system (DNS) configuration.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from this command:

```
>enable
#show dynamic-dns
eth 0/1:
 Hostname: host
 Is Updated: no
 Last Registered IP: 10.15.221.33
 Last Update Time: 00:00:00 UTC Thu Jan 01 1970
```


show dynamic-counter

Use the **show dynamic-counter** command to show statistics related to the dynamic counter. Variations of this command include:

show dynamic-counter
show dynamic-counter average-rates
show dynamic-counter <*slot/index*>

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

average-rates	Displays the average rate of frames/packets per second and bits per second assigned to a queue for the last 30 seconds and 5 minutes.
<*slot/index*>	Specifies the slot and port of the dynamic counter in the format <*slot/index*>. For example, **0/1**.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.
Release R13.3.0	Command was expanded to include the **average-rates** parameter.

Usage Examples

The following is sample output from this command:

>enable
#show dynamic-counter

Counter	Type	Port/Queue	Bytes	Packets	Avg Rate (kbps)	Status
0/1	TX	Gig Eth 1/Q 4	74984320	1171630	5	ACTIVE
0/2	CONGEST	Gig Eth 1/Q 4	0	0	0	ACTIVE
0/3	TX	Gig Eth 1/Q 3	75062016	1172844	6	ACTIVE
0/4	CONGEST	Gig Eth 1/Q 3	0	0	0	ACTIVE
0/5	TX	Gig Eth 1/Q 2	74986752	1171668	5	ACTIVE
0/6	CONGEST	Gig Eth 1/Q 2	0	0	0	ACTIVE


```
0/7     | TX        | Gig Eth 1/Q 1 | 75063154   |1172856  | 6          | ACTIVE
0/8     | CONGEST   | Gig Eth 1/Q 1 | 0          |0        | 0          | ACTIVE
0/9     | TX        | Gig Eth 1/Q 0 | 110363758  |1581014  | 8          | ACTIVE
0/10    | CONGEST   | Gig Eth 1/Q 0 | 0          |0        | 0          | ACTIVE
0/11    | NONE      | NONE          | 0          |0        | 0          | N/A
...
```

show eps

Use the **show eps** command to show information related to the external power supply (EPS) power state. The output of this command indicates if an EPS is connected, if it is delivering power, the available power, and whether the EPS has failed.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.8.0	Command was introduced.

Usage Examples

The following is sample output from this command:

```
>enable
#show eps
VCID 1 EPS is connected
VCID 1 EPS is delivering 370 watts
VCID 1 EPS fans are working.
VCID 2 EPS is connected
VCID 2 EPS is delivering 370 watts
VCID 2 EPS fans are working.
```


show ethernet cfm association

Use the **show ethernet cfm association** command to display Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance association (MA) configuration and statistical information. Variations of this command include:

show ethernet cfm association
show ethernet cfm association *<domain name>*
show ethernet cfm association *<domain name>* *<association name>*
show ethernet cfm association *<domain name>* *<association name>* **detail**
show ethernet cfm association detail
show ethernet cfm association none *<association name>*
show ethernet cfm association none *<association name>* **detail**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<domain name>	Optional. Specifies that output is limited to associations in the specified domain.
<association name>	Optional. Specifies that output is limited to the specified association.
detail	Optional. Specifies the output is displayed in detail, rather than summary, format.
none	Optional. Specifies that no domain name is used.

Default Values

No default values are necessary for this command.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following is sample output from the **show ethernet cfm association** command:

```
>enable
#show ethernet cfm association
---------------------------------------------------------------------------------------------------------------------
Index       Domain/Association                                  CCM     MEP-Cnt
                  Component   VID    Sender-ID
---------------------------------------------------------------------------------------------------------------------
1           Bogus/Test                                          1sec        0
1           BenchTest/BenchAssoc                                1min        3
                  giga-eth      0/2 0      none
```

The following is sample output from the **show ethernet cfm association detail** command:

```
>enable
#show ethernet cfm association detail
Domain Name: Bogus
Assoc Name: Test
  SNMP Index: 1
  CCM Interval: 1sec
  Components:
  MEP Count: 0

Domain Name: BenchTest
Assoc Name: BenchAssoc
  SNMP Index: 1
  CCM Interval: 1min
  Components:
    giga-eth 0/2 (VLAN=0, ID=none)
  MEP Count: 3
    1 (remote)
    2 (remote)
    3 (local)
```


show ethernet cfm domain

Use the **show ethernet cfm domain** command to display Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance domain (MD) configuration and statistical information. Variations of this command include:

show ethernet cfm domain
show ethernet cfm domain <*domain name*>
show ethernet cfm domain <*domain name*> **detail**
show ethernet cfm domain detail
show ethernet cfm domain none

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*domain name*>	Optional. Specifies that output is limited to associations in the specified domain.
detail	Optional. Specifies the output is displayed in detail, rather than summary, format.
none	Optional. Specifies that no domain name is used.

Default Values

No default values are necessary for this command.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following is sample output from the **show ethernet cfm domain** command:

```
>enable
#show ethernet cfm domain
---------------------------------------------------------------------------------------------
Index  Domain                                Lvl          Assoc-Count
---------------------------------------------------------------------------------------------
1      Bogus                                 5            1
2      BenchTest                             5            1
```

The following is sample output from the **show ethernet cfm domain detail** command:

```
>enable
#show ethernet cfm domain detail
Domain Name: Bogus
 SNMP Index:   1
 Level:        5
 Associations: 1
    test

Domain Name: BenchTest
 SNMP Index:   2
 Level:        5
 Associations: 1
    BenchAssoc
```


show ethernet cfm mep local

Use the **show ethernet cfm mep local** command to display configuration and statistical information for all Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoints (MEPs) configured on the system. Variations of this command include:

show ethernet cfm mep local
show ethernet cfm mep local detail
show ethernet cfm mep local domain *<domain name>* **association** *<association name>*
show ethernet cfm mep local fault
show ethernet cfm mep local interface *<interface>*
show ethernet cfm mep local mep-id *<mep id>*
show ethernet cfm mep local statistics

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Optional. Specifies the format is in detail, rather than summary, format.
domain *<domain name>*	Optional. Specifies that output is limited to MEPs in the specified domain.
association *<association name>*	Optional. Specifies that output is limited to MEPs in the specified association.
fault	Optional. Specifies that output is limited to only MEP fault information.
interface *<interface>*	Optional. Specifies that output is limited to the MEPs configured on the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id. subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.
mep-id *<mep id>*	Optional. Specifies that output is limited to MEPs with the specified ID. MEP ID range is **1** to **8191**.
statistics	Optional. Specifies that only MEP statistics are displayed.

Default Values

No default values are necessary for this command.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following is sample output from the **show ethernet cfm mep local detail** command:

```
>enable
#show ethernet cfm mep local detail
MEPs configured on this device

MEP-ID:       3
Domain/Assoc: BenchTest/Test
Mac Address:  00:A0:C9:00:D8:B2  Interface: giga-eth 0/2  Vlan:    0
Level:        5                  Direction: down         Priority: 7
Admin State:  up                 CCM State: yes

Fault Notification Settings
-----------------------------------------------
Highest Allowed Defect: MacStatus
AlarmTime: 2500 ms     ResetTime: 10000 ms
SNMP Trap: Disabled

Current Fault State
-----------------------------------
Fault State: Defect    Last Reported Fault: 08:41 PM, 09/16/2008

Current Highest Defect: None
Current Defects (Highest to Lowest defect priority):
    Xcon CCM:  -
    Err'd CCM: -
    Remote CCM: -
    MAC Status: -
    RDI:       -

Message Statistics
-----------------------------------
CCMs Transmitted:   2787   CCMs Received Out of Sequence: 4
LBRs Transmitted:   0          Next LBM ID:                36
LBRs Received:      30         LBRs Received Out of Order:  0
```



```
LBRs with bad data: 0
Next LTM ID:        1               Unexpected LTRs:            0
```

The following is sample output from the **show ethernet cfm mep local fault** command:

```
>enable
#show ethernet cfm mep local fault
MEPs configured on this device

MEP-ID:       3
Domain/Assoc: BenchTest/Test
Mac Address:  00:A0:C9:00:D8:B2  Interface: giga-eth 0/2  Vlan:    0
Level:        5                  Direction: down          Priority: 7
Admin State:  up                 CCM State: yes

Fault Notification Settings
-------------------------------------------------
Highest Allowed Defect: MacStatus
AlarmTime: 2500 ms      ResetTime: 10000 ms
SNMP Trap: Disabled

Current Fault State
---------------------------------------
Fault State: Defect     Last Reported Fault: 08:41 PM, 09/16/2008

Current Highest Defect: None
Current Defects (Highest to Lowest defect priority):
    Xcon CCM:   -
    Err'd CCM: -
    Remote CCM: -
    MAC Status: -
    RDI:
```


show ethernet cfm mep remote

Use the **show ethernet cfm mep remote** command to display configuration and statistical information for all remote Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoints (MEPs) stored on the system. Variations of this command include:

show ethernet cfm mep remote
show ethernet cfm mep remote domain <*domain name*> **association** <*association name*>
show ethernet cfm mep remote domain none association <*association name*>
show ethernet cfm mep remote interface <*interface*>
show ethernet cfm mep remote level <*level*>
show ethernet cfm mep remote local-mep <*mep id*>
show ethernet cfm mep remote remote-mep <*mep id*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

domain <*domain name*>	Optional. Specifies that output is limited to MEPs in the specified domain.
none	Optional. Specifies no domain name is used.
association <*association name*>	Optional. Specifies that output is limited to MEPs in the specified association.
interface <*interface*>	Optional. Specifies that output is limited to the MEPs configured on the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.
level <*level*>	Optional. Specifies that output is limited to MEPs in the specified maintenance level. Levels range from **0** to **7**.
local-mep <*mep id*>	Optional. Specifies that output is limited to the remote MEPs for all local MEPs with the specified ID. MEP ID range is **1** to **8191**.
remote-mep <*mep id*>	Optional. Specifies that output is limited to the remote MEPs with the specified ID. MEP ID range is **1** to **8191**.

Default Values

By default, all remote MEPs for all local MEPs are displayed.

By default, MEPs in all levels are displayed.

By default, all remote MEPs are displayed.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following is sample output from the **show ethernet cfm mep remote** command:

```
>enable
#show ethernet cfm mep remote
Local MEP 3
 Domain/Assoc: BenchTest/BenchAssoc
 Level: 5   VLAN: 0
 Interface: giga-eth 0/2
 Remote MEPs: (* = static)

   ID    State  Age       MAC                       RDI  Port     Iface
  ------------------------------------------------------------------------------------------------------------
 * 1     Ok     165936    00:A0:C8:1F:CE:B0          -   No TLV   Up
 * 2     Ok     165936    00:A0:C8:00:62:F2          -   No TLV   Up
```

show ethernet cfm stack

Use the **show ethernet cfm stack** command to display statistics and information about the Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) stack. Variations of this command include:

show ethernet cfm stack
show ethernet cfm stack interface *<interface>*
show ethernet cfm stack level *<level>*
show ethernet cfm stack vlan *<vlan id>*
show ethernet cfm stack vlan none

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interface *<interface>*	Optional. Specifies that output is limited to the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id. subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.
level *<level>*	Optional. Specifies that output is limited a specified maintenance level. Levels range from **0** to **7**.
vlan *<vlan id>*	Optional. Specifies that output is limited to a specific virtual local area network (VLAN). VLAN ID range is **1** to **4095**.
none	Optional. Specifies that output is limited to all VLANs.

Default Values

By default, all interfaces are displayed.

By default, all maintenance levels are displayed.

By default, all VLANs are displayed.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following is sample output from the **show ethernet cfm stack** command:

```
>enable
#show ethernet cfm stack
0-----------1-------------2-------------3-------------4-------------5-------------6-----------7-------------8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
-------------------------------------------------------------------------------------------------------------------------
Interface     Vlan      Lvl       Domain/Assoc
                          MEPID          MAC
-------------------------------------------------------------------------------------------------------------------------
eth 0/1       0         7         Domain_1/MA_1
                          1              00:A0:C8:16:96:0D
eth 0/2       20        5         Domain1/Assoc2
                          2012           00:0a:c8:00:01:03
```

show ethernet lmi

Use the **show ethernet lmi** command to display Ethernet local management interface (E-LMI) statistics and configuration information. Variations of this command include:

show ethernet lmi current
show ethernet lmi current *<interface>*
show ethernet lmi statistics
show ethernet lmi statistics *<interface>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

current	Specifies the current status of EVCs that will be sent out with the next E-LMI message are displayed.
statistics	Specifies the E-LMI statistics are displayed.
<interface>	Optional. Limits output to a specified E-LMI interface. Specify interfaces in the format *<interface type [slot/port]>*. For example, for a Gigabit Ethernet interface, use **gigabit eth 0/1**. Type **show ethernet lmi statistics ?** for a complete list of interfaces.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced.
Release R11.6.0	Command was expanded to include the **current** parameter.
Release R13.11.0	The output of this command was expanded to include ELMI forwarding status.

Usage Examples

The following example displays E-LMI statistics for the Gigabit Ethernet interface:

```
>enable
#show ethernet lmi statistics gigabit-ethernet 0/1
E-LMI Statistics for giga-eth 0/1
E-LMI Admin Status: Up
E-LMI Operation Status: Up
```



```
E-LMI Forwarding Status: Enabled
    UNI ID: giga-eth 0/1
    Reliability Errors:          0
Status Inquiry Timeouts:         0
Invalid Sequence Number:         0
Invalid Status Request:          0
Protocol Errors:                 0
Short Message:                   0
Invalid Version:                 0
Invalid Message Type:            0
Invalid Mandatory IE:            0
Mandatory IE Missing:            0
Out of Sequence IE:              0
Duplicated IE:                   0
Mandatory IE Missing:            0
Unexpected Recognized IE:        0

Last Full Status Inquiry Received:          00:50:35
Last Full Status Sent:                      00:50:35
Last Status Check Inquiry Received:         00:00:06
Last Status Check Sent:                     00:00:06
Last clearing of counters:                  never
```

show ethernet loopback

Use the **show ethernet loopback** command to display the status and ouput of facility or terminal loopback objects. Facility loopback objects are used to provision facility media access control (MAC) swap loopback tests and terminal loopback objects are used to provision Carrier Ethernet Terminal Loopback tests. Variations of this command include:

show ethernet loopback facility
show ethernet loopback facility *<name> <slot>*
show ethernet loopback facility slot *<slot>*
show ethernet loopback terminal
show ethernet loopback terminal *<name> <slot>*
show ethernet loopback terminal slot *<slot>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

facility	Specifies the output is for facility loopback objects.
terminal	Specifies the output is for terminal loopback objects.
<name>	Optional. Specifies that output is limited to the facility or terminal loopback object with the specified name.
<slot>	Optional. Specifies that output is limited to the facility or terminal loopback object with the specified slot.
slot *<slot>*	Optional. Specifies that output is limited to all facility or terminal loopback objects on a specified slot.

Default Values

By default, the status and output of all facility or terminal loopback objects are displayed.

Command History

Release R11.1.0	Command was introduced.
Release R13.7.0	Command was expanded to include the **terminal** loopback parameter.

Functional Notes

For more information regarding facility loopback objects and facility MAC swap loopback, refer to *Facility MAC Swap Loopback Command Set on page 3742*.

For more information regarding Carrier Ethernet Terminal Loopback objects, refer to *Carrier Ethernet Terminal Loopback Command Set on page 3739*.

Usage Examples

The following is sample output from the **show ethernet loopback facility** command:

>**enable**
#show ethernet loopback facility FACILITY 0

eth-lbk-fac “FACILITY” 0 is Enabled and Running
Matched S-tag : 100
Matched P-bit : na
Matched MAC : DA 00:A0:C8:00:00:01
System MAC : false
Interface : Gigabit Ethernet 0/1

show ethernet oam

Use the **show ethernet oam** command to display local and remote configuration and statistical information for Ethernet Link operations, administration, and maintenance (OAM) parameters stored on the system. Variations of this command include:

show ethernet oam discovery
show ethernet oam discovery interface *<interface>*
show ethernet oam statistics
show ethernet oam statistics interface *<interface>*
show ethernet oam status
show ethernet oam status interface *<interface>*
show ethernet oam summary

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

discovery	Displays discovery state information between the local OAM client and the remote peer. If no interface is specified, then information about all interfaces with Ethernet Link OAM enabled is displayed.
statistics	Displays Ethernet Link OAM Protocol Data Unit (PDU) counters by type, critical link fault records, and link-monitor event logs on a per-interface basis. If no interface is specified, then PDU information for all interface with Ethernet Link OAM enabled is displayed.
status	Displays the configured Ethernet Link OAM settings, including link-monitor settings, on a per-interface basis. If no interface is specified, then configuration for all interfaces with Ethernet Link OAM enabled is displayed.
summary	Displays a summary of the remote peer's configuration and capabilities for all interfaces that have Ethernet Link OAM enabled.
interface *<interface>*	Optional. Specifies that output is limited to the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id. subinterface id]>*. For example, for a Gigabit Ethernet interface, use **giga-eth 0/1**. For an Ethernet in the first mile (EFM) group, use **efm-group 1/1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following is sample output from the **show ethernet oam summary** command:

```
>enable
#show ethernet oam summary
Capability codes: L - Link Monitor, R- Remote Loopback
U - Unidirection, V - Variable Retrieval

Local           Remote
Interface       MAC Address       OUI      Mode      Capability
giga-eth 0/1    00:a0:c8:01:02:03 00A0C8   active    L V
```

The following is sample output from the **show ethernet oam discovery** command:

```
>enable
#show ethernet oam discovery
giga-eth 0/1

    Local Client
    ----------------
    Administrative configurations:
        Mode: active
        Unidirection: not supported
        Link monitor: not supported
        Remote loopback: not supported
        MIB retrieval: not supported
        Mtu size: 1518

    Operational status:
        Port status: UP
        Discovery state: Send Any
        PDU state: Any
        Stable: true
        Satisfied: true

    Remote client
    ------------------
    MAC address: 00:A0:C8:00:00:01
    Vendor (oui): 00A0C8
```

```
Administrative configuration:
    Mode: active
    Unidirection: not supported
    Link monitor: supported
    Remote loopback: not supported
    MIB retrieval: supported
    Mtu size: 1518

Operational status:
    Stable: true
    State valid: true
```


show ethernet y1731 file-save

Use the **show ethernet y1731 file-save** command to display a specified Y.1731 performance monitoring log file. Variations of this command include:

show ethernet y1731 file-save *<filename>*
show ethernet y1731 file-save current frame-delay two-way
show ethernet y1731 file-save current frame-loss single-ended
show ethernet y1731 file-save current frame-loss synthetic single-ended

Syntax Description

<filename>	Specifies the filename of the file to be displayed.
current	Specifies that the current file of the specified type should be displayed.
current frame-delay two-way	Specifies that the current frame-delay two-way (ETH-DM) log file should be displayed.
current frame-loss single-ended	Specifies that the current single-ended frame-loss (ETH-LM) log file should be displayed.
current frame-loss synthetic single-ended	Specifies that the current single-ended synthetic frame-loss (ETH-SLM) log file should be displayed.

Default Values

No default values are necessary for this command.

Command History

Release 11.6.0	Command was introduced.

Usage Examples

The following example displays the contents of the current ETH-LM log file:

(config)**#show ethernet y1731 file-save current frame-loss single-ended**
Current LM Session Data:

Single-Ended Loss Measurement Data Set
Fileformat Version: 1.02
EVC.Name |EVC.VLAN-ID|EVC.PCP|Device.Serial|Dest.MAC|LM.period|LM.TestID|LM.Suspect|
LM.Start_ToD|LM.End_ToD|LM.PDU-sent|LM.PDU-received|LM.Forward.TX.framecount|LM.Forward.RX.f
ramecount|LM.Backward.TX.framecount|LM.Backward.RX.framecount

show ethernet y1731 linktrace-cache

Use the **show ethernet y1731 linktrace-cache** command to display information for the Ethernet operations, administration, and maintenance (OAM) over Y.1731 linktrace cache.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display Ethernet OAM CFM over Y.1731 linktrace cache information:

>enable
#show ethernet y1731 linktrace-cache

show ethernet y1731 meg

Use the **show ethernet y1731 meg** command to display information for the Ethernet operations, administration, and maintenance (OAM) over Y.1731 maintenance entity group (MEG). Variations of this command include:

show ethernet y1731 meg
show ethernet y1731 meg char-string <*string*>
show ethernet y1731 meg icc-umc <*string*>

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

char-string <*string*>	Optional. Displays information for a MEG specified using a character string.
icc-umc <*string*>	Optional. Displays information for MEG specified using an ITU-Carrier Code Unique MEG ID Code (ICC-UMC).

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display information about all configured MEGs:

```
>enable
#show ethernet y1731 meg
```


show ethernet y1731 mep local

Use the **show ethernet y1731 mep local** command to display configuration and statistical information for all local Ethernet operations, administration, and maintenance (OAM) over Y.1731 maintenance endpoints (MEPs) configured on the system. Variations of this command include:

show ethernet y1731 mep local
show ethernet y1731 mep local detail
show ethernet y1731 mep local down
show ethernet y1731 mep local down statistics
show ethernet y1731 mep local interface <*interface*>
show ethernet y1731 mep local interface <*interface*> **statistics**
show ethernet y1731 mep local level <*level*>
show ethernet y1731 mep local level <*level*> **statistics**
show ethernet y1731 mep local meg char-string <*string*>
show ethernet y1731 mep local meg icc-umc <*string*>
show ethernet y1731 mep local mep-id <*id*>
show ethernet y1731 mep local mep-id <*id*> **statistics**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Optional. Displays information in detailed, rather than summary, format.
down	Optional. Displays the output limited to downstream MEPs.
interface <*interface*>	Optional. Displays the output limited to the MEPs configured on the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.
level <*level*>	Optional. Displays the output limited to MEPs with the specified level. Valid range is **0** to **7**.
meg char-string <*string*>	Optional. Displays the output limited to the maintenance entity group (MEG) specified with a character string.
meg icc-umc <*string*>	Optional. Displays the output limited to the MEG specified with an ITU-Carrier Code Unique MEG ID Code (ICC-UMC).
mep-id <*mep id*>	Optional. Displays the output limited to MEPs with the specified ID. MEP ID range is **1** to **8191**.
statistics	Optional. Displays only MEP statistics.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display information for all configured local MEPs:

```
>enable
#show ethernet y1731 mep local
```

show ethernet y1731 mep remote

Use the **show ethernet y1731 mep remote** command to display configuration and statistical information for all remote Ethernet operations, administration, and maintenance (OAM) over Y.1731 maintenance endpoints (MEPs) configured on the system. Variations of this command include:

show ethernet y1731 mep remote
show ethernet y1731 mep remote detail
show ethernet y1731 mep remote down
show ethernet y1731 mep remote down statistics
show ethernet y1731 mep remote interface <*interface*>
show ethernet y1731 mep remote interface <*interface*> **statistics**
show ethernet y1731 mep remote level <*level*>
show ethernet y1731 mep remote level <*level*> **statistics**
show ethernet y1731 mep remote meg char-string <*string*>
show ethernet y1731 mep remote meg icc-umc <*string*>
show ethernet y1731 mep remote mep-id <*id*>
show ethernet y1731 mep remote mep-id <*id*> **statistics**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Optional. Displays information in detailed, rather than summary, format.
down	Optional. Displays the output limited to downstream MEPs.
interface <*interface*>	Optional. Displays the output limited to the MEPs configured on the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id. subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.
level <*level*>	Optional. Displays the output limited to MEPs with the specified level. Valid range is **0** to **7**.
meg char-string <*string*>	Optional. Displays the output limited to the maintenance entity group (MEG) specified with a character string.
meg icc-umc <*string*>	Optional. Displays the output limited to the MEG specified with an ITU-Carrier Code Unique MEG ID Code (ICC-UMC).
mep-id <*mep id*>	Optional. Displays the output limited to MEPs with the specified ID. MEP ID range is **1** to **8191**.
statistics	Optional. Displays only MEP statistics.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display information for all configured remote MEPs:

>**enable**
#show ethernet y1731 mep remote

show ethernet y1731 stack

Use the **show ethernet y1731 stack** command to display statistics and information about the Ethernet operations, administration, and maintenance (OAM) over Y.1731 stack. Variations of this command include:

show ethernet y1731 stack
show ethernet y1731 stack interface *<interface>*
show ethernet y1731 stack level *<level>*
show ethernet y1731 stack vlan *<vlan id>*
show ethernet y1731 stack vlan none

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interface *<interface>*	Optional. Displays the output limited to the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id. subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interface, enter **interface ?** at the prompt.
level *<level>*	Optional. Displays the output limited to the specified maintenance level. Levels range from **0** to **7**.
vlan *<vlan id>*	Optional. Displays the output limited to the specified virtual local area network (VLAN). VLAN ID range is **1** to **4095**.
none	Optional. Displays no output for VLANs.

Default Values

By default, all interfaces are displayed.

By default, all maintenance levels are displayed.

By default, all VLANs are displayed.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to view all Ethernet OAM Y.1731 stack information:

>**enable**
#show ethernet y1731 stack

show evc

Use the **show evc** command to display configuration information for Ethernet virtual connections (EVCs) and EVC maps. Variations of this command include:

show evc
show evc <*name*>
show evc <*name*> **counters**
show evc <*name*> **counters** <*queue*>
show evc <*name*> **counters** <*queue*> **performance-statistics 15-minute**
show evc <*name*> **counters** <*queue*> **performance-statistics 15-minute** <*value*>
show evc <*name*> **counters** <*queue*> **performance-statistics 24-hour**
show evc <*name*> **counters** <*queue*> **performance-statistics 24-hour** <*value*>
show evc <*name*> **counters performance-statistics 15-minute**
show evc <*name*> **counters performance-statistics 15-minute** <*value*>
show evc <*name*> **counters performance-statistics 24-hour**
show evc <*name*> **counters performance-statistics 24-hour** <*value*>
show evc-map
show evc-map <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

evc <*name*>	Optional. Specifies that information for a specific EVC is displayed. If no name is specified, information for all EVCs is displayed.
evc-map <*name*>	Optional. Specifies that information for a specific EVC map is displayed. If no name is specified, information for all EVC maps is displayed.
counters	Optional. Displays Metro Ethernet Forum (MEF) counters for the specified EVC.
counters <*queue*>	Optional. Displays MEF counters for the specified queue number on the MEN port associated with the EVC. Valid entry for <*queue*> is **0** through **7**.
performance-statistics	Optional. Displays aggregate performance statistics.
15-minute	Optional. Displays the statistics for a 15-minute period in the last 24 hours.
24-hour	Optional. Displays the statistics for a 24-hour period in the last 7 days.
<*value*>	Optional. Specifies which 15-minute period in the last 24 hours or which 24-hour period in the last 7 days is displayed. Range for 15-minute periods is **1** to **96**; range for 24-hour periods is **1** to **7**.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.
Release R11.5.0	Command was expanded to include **counters** and **performance-statistics** parameters.
Release R13.11.0	Output of the **show evc** <*name*> **counters** command was changed to include ingress and egress Layer 2 bytes collected on both the UNI and NNI interfaces and displayed on a per-EVC and per-CoS (queue) basis. UNI and NNI Layer 2 bytes are displayed in **Total Egress Bytes** and **Total Ingress Bytes** output lines beneath the aggregate counters for the EVC or CoS queue. In addition, **Ingress Red Bytes** and **Ingress Yellow Discard Bytes** have also been included in the command output.

Usage Examples

The following is sample output from the command to display information for all configured EVCs:

```
>enable
#show evc
All EVC Tags Available in MEN
EVC evc1
    S-TAG                    : --
    Admin State              : Disabled
    EVC Status               : Not Running - Disabled
    CE-VLAN Preservation     : Enabled
```

The following example displays 15-minute interval performance statistics for **EVC-200** in queue 1:

```
# show evc EVC-200 counters 0 performance-statistics 15-minute 1
EVC-200 Queue 0 15-Minute PM (1)
07:00
  Ingress Green Frames           :  0
  Ingress Green Bytes            :  0
  Ingress Green Discard Frames   :  0
  Ingress Green Discard Bytes    :  0
  Egress Green Frames            :  0
  Egress Green Bytes             :  0
  Egress Green Discard Frames    :  0
  Egress Green Discard Bytes     :  0
```

show event-history

Use the **show event-history** command to display all entries in the current local event-history log.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The event history provides useful information regarding the status of the system and individual port states. Use the event history as a troubleshooting tool when identifying system issues. The following is sample output from the event-history log.

```
>enable
#show event-history
Using 526 bytes
2002.07.12 15:34:01 T1.t1 1/1 Yellow
2002.07.12 15:34:01 INTERFACE_STATUS.t1 1/1 changed state to down.
2002.07.12 15:34:02 T1.t1 1/1 No Alarms
2002.07.12 15:34:02 INTERFACE_STATUS.t1 1/1 changed state to up.
2002.07.12 15:34:03 INTERFACE_STATUS.eth 0/1 changed state to up.
2002.07.12 15:34:10 OPERATING_SYSTEM Warm Start
2002.07.12 15:34:12 PPP.NEGOTIATION LCP up
2002.07.12 15:34:12 PPP.NEGOTIATION IPCP up
```


show fan-tach

Use the **show fan-tach** command to view the unit's current fan speed.

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows the current fan speed on an AOS device with two chassis fans:

```
>enable
#show fan-tach
Fan Tach (in Percent)    %
Chassis Fan 1            45
Chassis Fan 2            45
```

The following example shows the current fan speed on an AOS device with one central fan:

```
>enable
#show fan-tach
Fan Tach (in Percent)    %
Central Fan              59
```


show file

Use the **show file** command to display a specified file to the terminal screen. Variations of this command include:

show file *<filename>*
show file *<filename>* **checksum**
show file cflash *<filename>*
show file cflash *<filename>* **checksum**
show file flash *<filename>*
show file flash *<filename>* **checksum**
show file ramdisk *<filename>*
show file ramdisk *<filename>* **checksum**
show file usbdrive0 *<filename>*
show file usbdrive0 *<filename>* **checksum**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*To display files located in the flash memory on products with CompactFlash® capability, the **flash** keyword must be specified whether or not a CompactFlash card is installed.*

*Not all units are capable of using a RAM disk file system or have a CompactFlash card installed. Use the **show file ?** command to display a list of valid commands at the enable prompt.*

The contents of the file are displayed only if the file is less than 300 kilobytes.
The checksum is displayed only if the file is less than 500 kilobytes.

Syntax Description

<filename>	Displays information on the specified file. Wildcard entries (such as ***.biz**) are not valid for the **show file** command.
cflash	Specifies a file located in CompactFlash memory.
checksum	Optional. Displays the message digest 5 (MD5) checksum of the specified file.
flash	Specifies a file located in flash memory.

ramdisk	Specifies a file located in volatile RAM disk.
usbdrive0	Specifies a file located in Universal Serial Bus (USB) flash drive memory.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 12.1	Command was expanded to include the **cflash** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include the **usbdrive0** parameter.

Usage Examples

The following is sample output from the **show file cflash** command:

```
>enable
#show file cflash startup-config
Router#show file startup-config
Using 2558 bytes
!
!
hostname “Router”
enable password password
!
clock timezone -6-Central-Time
!
ip subnet-zero
ip classless
ip routing
!
no auto-config
!
event-history on
no logging forwarding
no logging email
logging email priority-level info
!
no service password-encryption
!
username “admin” password “password”
!
--MORE--
```


The **show file ramdisk** command issues the following error message if the file is greater than 300 kilobytes:

>**enable**
#show file ramdisk NV3130A-17-07-00-26-AE.biz
%Cannot show files larger than 300000 bytes.

The following is sample **show file ramdisk** <*filename*> **checksum** output:

>**enable**
#show file ramdisk default-config.txt checksum
AA02EC815B93B0E41C738A71C6AFCBC4

show flash

Use the **show flash** command to display a list of all files currently stored in flash memory. Variations of this command include:

show flash
show flash *<filename>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<filename>	Optional. Displays details for a specified file located in flash memory. Enter a wildcard (such as ***.biz**) to display the details for all files matching the entered pattern.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show flash** command:

```
>enable
#show flash
Files:
 245669 010100boot.biz
1141553 new.biz
    821 startup-config
   1638 startup-config.old
1175679 020016.biz
    821 startup-config.bak
2572304 bytes used 4129776 available 6702080 total
System image file is “020100.biz”
```


show frame-relay

Use the **show frame-relay** command to display configuration and status parameters for configured virtual Frame Relay interfaces. Variations of this command include the following:

show frame-relay lmi
show frame-relay pvc
show frame-relay pvc interface frame-relay <*interface*>
show frame-relay pvc interface frame-relay <*interface*> **realtime**
show frame-relay pvc realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

lmi	Displays local management interface (LMI) statistics for each virtual Frame Relay interface.
pvc	Displays permanent virtual circuit (PVC) configuration and statistics for all virtual Frame Relay interfaces (or a specified interface).
interface frame-relay <*interface*>	Optional. Displays Frame Relay PVC statistics for a specific Frame Relay interface (for example, **fr 1**).
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 10.1	**Realtime** parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C)**. If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following are sample outputs from various **show frame-relay** commands:

```
>enable
#show frame-relay lmi
LMI statistics for interface FR 1 LMI TYPE = ANSI
Num Status Enq. Sent 79       Num Status Msgs Rcvd 71
Num Update Status Rcvd 12     Num Status Timeouts 5

>enable
#show frame-relay pvc
Frame Relay Virtual Circuit Statistics for interface FR 1
              Active      Inactive      Deleted      Static
local         2           0             0            2
DLCI = 16 DLCI USAGE = LOCAL PVC STATUS = ACTIVE INTERFACE = FR 1.16
MTU: 1500
input pkts: 355                 output pkts: 529              in bytes: 23013
out bytes: 115399               dropped pkts: 13              in FECN pkts: 0
in BECN pkts: 0                 in DE pkts: 0                 out DE pkts: 0
pvc create time: 00:00:00:12    last time pvc status changed: 00:00:13:18
DLCI = 20 DLCI USAGE = LOCAL PVC STATUS = ACTIVE INTERFACE = FR 1.20
MTU: 1500
input pkts: 0                   output pkts: 44               in bytes: 0
out bytes: 22384                dropped pkts: 11              in FECN pkts: 0
in BECN pkts: 0                 in DE pkts: 0                 out DE pkts: 0
pvc create time: 00:00:01:25    last time pvc status changed: 00:00:13:18
```


show frame-relay fragment

Use the **show frame-relay fragment** command to display detailed fragmentation statistics for Frame Relay subinterfaces with FRF.12 fragmentation enabled. Variations of this command include:

show frame-relay fragment
show frame-relay fragment interface frame-relay <*subinterface*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interface frame-relay <*subinterface*>	*Optional.* Displays detailed fragmentation statistics for the specified Frame Relay subinterface. Subinterfaces are expressed in the format *interface id.subinterface id* (for example, **fr 1.16**).

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following are sample outputs from various **show frame-relay fragment** commands:

>enable
#show frame-relay fragment

interface	dlci	frag_size	rx_frag	tx_frag	dropped_frag
fr 1.1	17	100	46	48	0
fr 1.2	18	200	42	21	0

>**enable**
#show frame-relay fragment frame-relay 1.1
DLCI = 17 FRAGMENT SIZE = 100

rx frag. pkts	46	tx frag. pkts	48
rx frag. bytes	4598	tx frag. bytes	4724
rx non-frag. pkts	18	tx non-frag. pkts	28
rx non-frag. bytes	1228	tx non-frag. bytes	1960
rx assembled pkts	23	tx pre-fragment pkts	34
rx assembled bytes	5478	tx pre-fragment bytes	6324
dropped reassembling pkts	0	dropped fragmenting pkts	0
rx out-of-sequence fragments	0		
rx unexpected beginning fragment	0		

show frame-relay multilink

Use the **show frame-relay multilink** command to display information associated with the Frame Relay multilink interface. Variations of this command include:

show frame-relay multilink
show frame-relay multilink detailed
show frame-relay multilink <*interface*>
show frame-relay multilink <*interface*> **detailed**
show frame-relay multilink interface frame-relay <*subinterface*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*interface*>	Optional. Specifies the display of information for a specific interface. Enter the **show frame-relay multilink ?** command for a complete list of interfaces.
detailed	Optional. Displays more detailed information.
interface frame-relay <*subinterface*>	Optional. Displays detailed fragmentation statistics for the specified Frame Relay subinterface. Subinterfaces are expressed in the format *interface id.subinterface id* (for example, **fr 1.16**).

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show frame-relay multilink** command:

>**enable**
#show frame-relay multilink
Bundle: frame-relay 1 is DOWN; class A bundle
Near-end BID: MFR1; Far-end BID: unknown

show garp timer

Use the **show garp timer** command to display the current configured Generic Attribute Registration Protocol (GARP) application timer values.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays the current configured GARP application timer values:

```
>enable
#show garp timer
Timer          Timer Value (milliseconds)
--------       --------------------------
Join            200
Leave           600
LeaveAll        10000
```


show global-policer

Use the **show global-policer** command to view virtual AOS (vAOS) global policer statistics.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R12.1.0	Command was introduced.

Functional Notes

vAOS global policer statistics reveal valuable information about the data usage of the vAOS instance as it relates to the license allocated bandwidth for the vAOS instance. Using this information can be beneficial in determining if data needs are being met by the current license limit or if a higher bandwidth license is necessary.

The policer statistics are gathered from the interface statistics of the policed interfaces. If an interface's counters are cleared, those statistics are not included in the number displayed in the command output. The current aggregate traffic rate is computed over the configured global rate interval, which applies to the rate statistics for all interfaces. This interval is configurable via the command *statistics rate-interval <value> on page 1863*.

Usage Examples

The following example displays all vAOS global policer statistics:

```
>enable
#show global-policer
Global Policer
    Licensed Aggregate Traffic Rate     : 50 Mbps
    Current Aggregate Traffic Rate      : 15 Mbps (5 minute rate)
    Committed Burst Size                : 5625000 bytes
    Dropped Packets                     :1000 packets
    Dropped Bytes                       : 64000 bytes
    Last Cleared Time                   : Mon Nov 23 16:43:51 CST 2015

    Warning Events
    Period                              : 5 minutes
    Rate Threshold                      : 90% of licensed rate
    Dropped Packet Threshold            : 10000 packets
```


show gvrp configuration

Use the **show gvrp configuration** command to show a GARP VLAN Registration Protocol (GVRP) configuration summary for the switch.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays a GVRP configuration summary for the switch:

```
>enable
#show gvrp configuration
Global GVRP Configuration:
GVRP Feature is currently enabled globally.
GVRP Timers (milliseconds)
Join 200
Leave 600
LeaveAll 20000
Port based GVRP Configuration:
GVRP enabled ports
---------------------------------------------------
eth 0/24

#
```


show gvrp statistics

Use the **show gvrp statistics** command to show statistics related to GARP VLAN Registration Protocol (GVRP). Variations of this command include:

show gvrp statistics
show gvrp statistics interface *<interface>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interface *<interface>*	Optional. Shows the information for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show gvrp statistics interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example displays statistics related to GVRP for Ethernet interface 0/24:

```
>enable
#show gvrp statistics interface ethernet 0/24
Name: eth 0/24
Join Empty Received: 0
Join In Received: 272
Empty Received: 30
Leave Empty Received: 0
```


show hmr

Use the **show hmr** command to display Session Initiation Protocol (SIP) header manipulation rules (HMR) statistics from traffic to which an HMR policy is applied. The output can be filtered based on policy, policy user, rule set, direction, and message type. In addition, you can sort the output by policy, policy user, rule set, direction, or message type. This command can be used to determine the activity of an HMR policy, where they policy is most used, and by whom. Variations of this command include:

show hmr
show hmr direction in
show hmr direction out
show hmr message-type request
show hmr message-type response
show hmr policy *<name>*
show hmr rule-set *<name>*
show hmr sort direction in
show hmr sort direction out
show hmr sort message-type request
show hmr sort message-type response
show hmr sort policy *<name>*
show hmr sort user
show hmr user global
show hmr user proxy-server
show hmr user proxy-user
show hmr user *<user>*

*Each of the **show hmr** command variations can be used multiple times within a single command. For example, you can display SIP HMR statistics for a specified policy and direction by entering **show hmr policy MYPOLICY1 direction in**.*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

direction in	Optional. Limits the command output to SIP HMR statistics for inbound SIP traffic.
direction out	Optional. Limits the command output to SIP HMR statistics for outbound SIP traffic.
message-type request	Optional. Limits the command output to SIP HMR statistics for request messages.

message-type response	Optional. Limits the command output to SIP HMR statistics for response messages.
policy <*name*>	Optional. Limits the command output to SIP HMR statistics for a specified HMR policy.
rule-set <*name*>	Optional. Limits the command output to SIP HMR statistics for a specified rule set.
sort	Optional. Sorts SIP HMR statistics by direction, message type, policy name, or policy user.
user global	Optional. Limits the command output to SIP HMR statistics for the SIP stack.
user proxy-server	Optional. Limits the command output to SIP HMR statistics for SIP proxy servers.
user proxy-user	Optional. Limits the command output to SIP HMR statistics for SIP proxy users.
user <*user*>	Optional. Limits the command output to SIP HMR statistics for a specified user.

Default Values

No default values necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example displays all HMR statistics:

>**enable**
#show hmr
Policy: MyPolicy1
Msgs Evaluated: 0
Msgs Altered: 0
User Application: Global inbound request

Rule Set	Message Rule	Action	Seq #	Count
Set 1	Rule1	Modify Variable	10	0
		Modify Variable	20	0
		Add Header	30	3
		Modify Header	40	2

show hosts

Use the **show hosts** command to display the contents of the domain naming system (DNS) host table. Output from this command displays both Internet Protocol version 4 (IPv4) and IPv6 entries, as well as separate server addresses for the DNS client and proxy. Variations of this command include:

show hosts
show hosts realtime
show hosts verbose
show hosts vrf <*name*>
show hosts vrf <*name*> **realtime**
show hosts vrf <*name*> **verbose**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

realtime	Optional. Displays information in real time.
verbose	Optional. Displays the details of the IP name, style, name servers, and host table entries without the truncation of long IP addresses and host names.
vrf <*name*>	Optional. Displays DNS information for the specified virtual routing and forwarding (VRF) instance. If no VRF instance is specified, host table information for the default VRF instance is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** <*name*> parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command was expanded to include both IPv4 and IPv6 entries in the output and the **realtime** keyword.

Functional Notes

The list below describes the fields contained in the DNS host table:

- Flags: Indicate whether the entry is permanent (perm) or temporary (temp).
- Age: Indicates the age of the entry.
- Type: Shows the protocol type as addresses (A) or service (SRV).
- Priority: 1 or 2.
- Address: Displays the IP address for the entry.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example is sample output from the **show hosts** command:

>**enable**
#show hosts

Name/address lookup uses domain name service
DNS Proxy is enabled
Name servers are 10.23.115.254
Current proxy server is 10.23.115.254
Current client server is 10.23.115.254

Host	Flags	Age	Type	Priority	Address/Alias
abc.com	temp	193	A		-2000:ef0a::1500:37af:362:ed
Archive.msstate.edu	temp	16907	A		-130.18.80.18
dns11.11nwd.net	temp	673	A		-200:a50:1a0e::1500:eddf

show http secure-server certificate

Use the **show http secure-server certificate** command to display information regarding HTTPS private key and certificates.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.7.0	Command was introduced.

Usage Examples

The following is sample output from the **show http secure-server certificate** command:

```
>enable
#show http secure-server certificate
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         70:a2:aa:7c:8e:d8:dd:b2:68:e1:58:65:55:84:69:81:19:91:7b:29
   Signature Algorithm: sha256WithRSAEncryption
      Issuer: C=US, ST=AL, L=Huntsville, O=Adtran, Inc., CN=NetVanta
      Validity
         Not Before: Jun 19 19:11:09 2015 GMT
         Not After : Jun 17 19:11:09 2023 GMT

-----BEGIN CERTIFICATE-----
MIIDbzCCAlegAwIBAgIUcKKqfI7Y3bJo4VhlVYRpgRmReykwDQYJKoZIhvcNAQEL
BQAwWTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkFMMRMwEQYDVQQHDApIdW50c3Zp
dHN2aWxsZTELMAkGA1UEBhMCVVMwHhcNMTUwNDI5MDY0ODE0WhcNMjMwNDI3MDY0
DTE1MDYxOTE5MTEwOVoXDTIzMDYxNzE5MTEwOVowWTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgMAkFMMRMwEQYDVQQHDApIdW50c3ZpbGxlMRUwEwYDVQQKDAxBRFRSQU4s
```


lEluYy4xETAPBgNVBAMMCE5ldFZhbnRhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA2x/r4499jQKrXX0810fTkIoGk5jNwkfQ7JkZxSoqX7OPzYSYQ8/E
1UF/fsv0SxlHCTVTVmihLSbkc75fDEs6NL3URGFXBLJJ/Rlg5g3UwdnpUR02GUr3
zP7kXP+UvcuUWD7DqamcD2eS/78sn6kZUVE+ocytr89KDsevU/eRhEvUq2Z3YgIA
3fg3hGYYD2vTSarWOmRd3cFxzw7C2TTUnHCVu+CCVxvOmETFljfHwjOl1KgBBTVe
o2rR+Yyb5RtUiPmyQdVeR8L6OBV0/yToF4/AX73gUiOjMOeiPZ30SQPIJhjumVvV
FC1w8CfHALoDjbpBGqwIuxO9XjqtIdxe7QIDAQABoy8wLTAMBgNVHRMBAf8EAjAA
MB0GA1UdDgQWBBTyhd5mKbpAOtV03ObopcGtuYFg8TANBgkqhkiG9w0BAQsFAAOC
AQEAk3E3ea3esaLf4KgbXvViBlT0/S9+P6gmU88hZcyr6/ArOzpSv0Ne21orByk3
OsBBFoGibMfOYzRL8tPD3b5aqqwjDlXmG2rg8i1W/tLDeyo6xDPrxJEN+3EEqLIP
3EKEVAyL1a6DaeQOvv3B5tN28mmLYCxP5749gcnE3jIH77cCxLrxR1HcvGlelecw
yi8RioKBho/yOl5jCR4VTgDYzXhbrdSheuVAsjoEb1yaNi00sKlJbfIneHlUfYK9
gD0rBw5hoW7QxSx7N/oo3D/7yKxN5aKyCAJwlfyRWeytSrVc9UgoXzD4PNu7UiYz
jtgSsHe4c5Vwx8xS+0G9ttf42w==
-----END CERTIFICATE-----

show hw-access-list

Use the **show hw-access-list** command to display hardware access control list (ACL) configuration and statistics. Variations of this command include:

show hw-access-list

show hw-access-list <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*name*>	Optional. Specifies a particular hardware ACL to display.

Default Values

No default values are necessary for this command.

Command History

Release 17.6	Command was introduced.

Functional Notes

The **show hw-access-list** command displays all configured hardware ACLs in the system. All entries in the ACL are displayed, and a counter indicating the number of frames matching the entry is listed.

Usage Examples

The following is sample output from the **show hw-access-list** <*name*> command, using the hardware ACL **NET135**:

```
>enable
#show hw-access-list NET135
Extended IP hardware access list NET135
  permit ip 10.22.135.0 0.0.0.255  any    log (302 matches)
  permit ip any  10.22.135.0 0.0.0.255    log (279 matches)
```


The following is sample output from the **show hw-access-list** command which displays information for all configured hardware ACLs:

```
>enable
#show hw-access-list
Extended IP hardware access list NET135
   permit ip 10.22.135.0 0.0.0.255  any    log (131 matches)
   permit ip any  10.22.135.0 0.0.0.255    log (110 matches)
Extended MAC hardware access list ADTN
  permit mac 00:a0:c8:00:00:00 00:00:00:ff:ff:ff any log (44055 matches)
  permit mac any 00:a0:c8:00:00:00 00:00:00:ff:ff:ff log (3011 matches)
```


show hw-access-map

Use the **show hw-access-map** command to display hardware access map configuration and statistics. Variations of this command include:

show hw-access-map
show hw-access-map *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Optional. Displays only the statistics for the named hardware access map.

Default Values

No default values are necessary for this command.

Command History

Release 17.6	Command was introduced.

Usage Examples

The following is sample output from the **show hw-access-map** *<name>* command, using the access map **HW-FILTER**:

```
>enable
#show hw-access-map HW-FILTER
Hardware Access Map HW-FILTER
  Forward: mac ADTN and ip NET135
  VLANs: 2-3
```


show hw-filter-resource

Use the **show hw-filter-resource** command to display the used and available hardware filter resources. This information is valuable when making changes to configured hardware access control lists (ACLs) and hardware access maps. For more information on hardware ACLs and access maps, refer to the *Hardware ACL and Access Map Command Set on page 4235*.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.6	Command was introduced.

Functional Notes

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria, an error message is displayed.

Usage Examples

The following is sample output from the **show hw-filter-resource** command:

```
>enable
#show hw-filter-resource
Total Rules: 512
Rules Used: 128
```


show interfaces

Use the **show interfaces** command to display configuration parameters and current statistics for all interfaces (or a specified interface). Variations of this command include the following:

show interfaces
show interfaces description
show interfaces status
show interfaces <*interface*>
show interfaces <*interface*> **extended**
show interfaces <*interface*> **performance-statistics**
show interfaces <*interface*> **performance-statistics** <*x-y*>
show interfaces <*interface*> **performance-statistics 15-minute**
show interfaces <*interface*> **performance-statistics 15-minute** <*value*>
show interfaces <*interface*> **performance-statistics 24-hour**
show interfaces <*interface*> **performance-statistics 24-hour** <*value*>
show interfaces <*interface*> **performance-statistics total-24-hour**
show interfaces <*interface*> **realtime**
show interfaces <*interface*> **verbose**
show interfaces <*interface*> **version**

*Not all subcommands apply to all interfaces or are available on all AOS units. Type **show interfaces** <interface> **?** for a list of valid subcommands for the specified interface. Some subcommands are only valid on AOS units with switchport or gigabit switchport interfaces. Enter the **show interfaces ?** command to display a list of valid subcommands for your specific platform.*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<interface>	Optional. Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show interfaces ?** for a complete list of valid interfaces.
description	Displays information, such as description, administrative status, line protocol status, and description for the interfaces.
status	Displays information, such as description, type, status, virtual local area network (VLAN), speed, and duplex for the interfaces. This subcommand is only available on AOS units with switchport or Gigabit-switchport interfaces.
extended	Optional. Displays extended medium attachment unit (MAU) statistics.
performance-statistics	Optional. Displays line performance statistics.
<x-y>	Optional. Shows a specified interval (x) or range of intervals (x-y). Valid range is 1 to 96.
total-24-hour	Optional. Displays the current 24-hour totals.
<value>	Optional. Specifies which 15-minute period in the last 24 hours or which 24-hour period in the last 7 days is displayed. Range for 15-minute periods is **1** to **96**; range for 24-hour periods is **1** to **7**.
15-minute	Optional. Displays the statistics for a 15-minute period in the last 24 hours.
24-hour	Optional. Displays the statistics for a 24-hour period in the last 7 days.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.
verbose	Optional. Displays detailed configuration information on the terminal screen (versus only the nondefault values).
version	Optional. Displays current version information (e.g., model and list number, software version, etc.) for the interface.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 6.1	Command was updated to include the **performance-statistics** parameter to display RFC 2662 line performance statistics.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 10.1	Command was expanded to include the **realtime** parameter. The primary rate interface (PRI) was also added.

Release 11.1	Command was expanded to include the **description**, **status**, and **verbose** parameters. The demand, foreign exchange office (FXO), and serial interfaces were also added.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the **realtime** and **extended** parameters. The Gigabit Ethernet interface was also added.
Release 18.3	Command was expanded to include the **extended** parameter.
Release R10.10.0	Command was expanded to include the Ethernet in the first mile (EFM) link and EFM group interfaces.
Release R10.11.0	Command was expanded to include the T4 interface.
Release R11.2.0	Command was expanded to include the very high-speed digital subscriber line (VDSL) interfaces.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.
Release R12.1.0	Command output was modified for virtual AOS (vAOS) instances.
Release 13.1.0	Command was expanded to include the virtual extensible local area network (VxLAN) tunnel interface.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show interfaces description** command:

```
>enable
#show interfaces description
Interface       Status          Protocol        Description
eth 0/1         Admin Up        Line Up         Desk 1
eth 0/2         Admin Up        Line Up         Desk 2
eth 0/3         Admin Up        Line Up         Desk 3
eth 0/4         Admin Up        Line Up         Desk 4
eth 0/5         Admin Up        Line Up         Desk 5
eth 0/6         Admin Up        Line Up         Desk 6
eth 0/7         Admin Up        Line Up         Desk 7
eth 0/8         Admin Up        Line Down       Desk 8
eth 0/9         Admin Up        Line Up         Desk 9
eth 0/10        Admin Up        Line Up         Desk 10
```


eth 0/11	Admin Up	Line Up	Desk 11
eth 0/12	Admin Up	Line Up	Desk 12
eth 0/13	Admin Up	Line Up	Desk 13
eth 0/14	Admin Up	Line Up	Desk 14
eth 0/15	Admin Up	Line Up	Desk 15
eth 0/16	Admin Up	Line Up	Desk 16
eth 0/17	Admin Up	Line Up	Desk 17
eth 0/18	Admin Up	Line Up	Desk 18
eth 0/19	Admin Up	Line Up	Desk 19
eth 0/20	Admin Up	Line Up	Desk 20
eth 0/21	Admin Up	Line Up	Desk 21
eth 0/22	Admin Up	Line Up	Desk 22
eth 0/23	Admin Up	Line Up	Desk 23
eth 0/24	Admin Up	Line Up	Desk 24
giga-eth 0/1	Admin Up	Line Up	Uplink Trunk
giga-eth 0/2	Admin Up	Line Down	Unused

The following is sample output from the **show interfaces status** command:

```
>enable
#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
eth 0/1		connected	trunk	a-full	a-100	10/100
eth 0/2		notconnected	trunk	?	?	10/100
eth 0/3		notconnected	trunk	?	?	10/100
eth 0/4		notconnected	trunk	?	?	10/100
eth 0/5		notconnected	trunk	?	?	10/100
eth 0/6		notconnected	trunk	?	?	10/100
eth 0/7		notconnected	trunk	?	?	10/100
eth 0/8		notconnected	trunk	?	?	10/100
eth 0/9		notconnected	trunk	?	?	10/100
eth 0/10		notconnected	trunk	?	?	10/100
eth 0/11		notconnected	trunk	?	?	10/100
eth 0/12		notconnected	trunk	?	?	10/100
eth 0/13		notconnected	trunk	?	?	10/100
eth 0/14		notconnected	trunk	?	?	10/100
eth 0/15		notconnected	trunk	?	?	10/100
eth 0/16		notconnected	trunk	?	?	10/100
eth 0/17		notconnected	trunk	?	?	10/100
eth 0/18		notconnected	trunk	?	?	10/100
eth 0/19		notconnected	trunk	?	?	10/100
eth 0/20		notconnected	trunk	?	?	10/100
eth 0/21		notconnected	trunk	?	?	10/100
eth 0/22		notconnected	trunk	?	?	10/100
eth 0/23		notconnected	trunk	?	?	10/100
eth 0/24		notconnected	trunk	?	?	10/100

giga-eth 0/1	notconnected	trunk	?	?	Gig
giga-eth 0/2	notconnected	trunk	?	?	Gig

The following are samples from various **show interfaces** commands:

```
>enable
#show interfaces t1 1/1
t1 1/1 is UP
 T1 coding is B8ZS framing is ESF
 Clock source is line FDL type is ANSI
 Line build-out is 0dB
 No remote loopbacks No network loopbacks
DS0 Status: 12345678901234567890123
            NNNNNNNNNNNNNNNNNNNNNNN
Line Status: -- No Alarms --
Current Performance Statistics:
   0 Errored Seconds 0 Bursty Errored Seconds
   0 Severely Errored Seconds 0 Severely Errored Frame Seconds
   0 Unavailable Seconds 0 Path Code Violations
   0 Line Code Violations 0 Controlled Slip Seconds
   0 Line Errored Seconds 0 Degraded Minutes

#show interfaces modem 1/2
modem 1/2 is UP
 Line status: on-hook
 Caller ID will be used to route incoming calls
   0 packets input 0 bytes 0 no buffer
   0 runts 0 giants 0 throttles
   0 input errors 0 CRC 0 frame
   0 abort 0 ignored 0 overruns
   0 packets output 0 bytes 0 underruns
   0 input clock glitches 0 output clock glitches
   0 carrier lost 0 cts lost

#show interfaces eth 0/1
Ip address is 10.200.1.50
 Netmask is 255.255.0.0
 MTU is 1500
 Fastcaching is Enabled
 RIP Authentication is Disabled
 RIP Tx uses global version value
 RIP Rx uses global version value

#show interfaces dds 1/1
dds 1/1 is UP line protocol is UP
 Encapsulation FRAME-RELAY (fr 1)
```



```
 Loop rate is set to 56000 actual rate is 56000
 Clock source is line
 Data scrambling is disabled
 No Loopbacks
    75 packets input 6108 bytes 0 no buffer
    0 runts 0 giants 0 throttles
    0 input errors 0 CRC 0 frame
    0 abort 0 ignored 0 overruns
    81 packets output 11496 bytes 0 underruns
    0 input clock glitches 0 output clock glitches
    0 carrier lost 0 cts lost
```

#show interfaces fr 1

```
TDM group 10 line protocol is UP
Encapsulation FRAME-RELAY (fr 1)
    463 packets input 25488 bytes 0 no buffer
    0 runts 0 giants 0 throttles
    0 input errors 0 CRC 0 frame
    0 abort 0 ignored 0 overruns
    864 packets output 239993 bytes 0 underruns
    0 input clock glitches 0 output clock glitches
    0 carrier lost 0 cts lost
Line Status: -- No Alarms --
Current Performance Statistics:
    0 Errored Seconds 0 Bursty Errored Seconds
    0 Severely Errored Seconds 0 Severely Errored Frame Seconds
    0 Unavailable Seconds 0 Path Code Violations
    0 Line Code Violations 0 Controlled Slip Seconds
    0 Line Errored Seconds 0 Degraded Minutes
```

#show interfaces fr 1.100

```
fr 1.100 is Active
Ip address is 63.97.45.57, mask is 255.255.255.248
Interface-dlci is 100
MTU is 1500 bytes, BW is 96000 Kbit (limited)
Average utilization is 53%
```

#show interfaces shdsl 1/1

```
shdsl 1/1 is UP, line protocol is DOWN
 Encapsulation FRAME-RELAY IETF (fr 1)
 Equipment type is cpe
 Line rate is 2056kbps
 No alarms.
 SHDSL training complete. EOC is up.
 No local loopbacks, No remote loopbacks
 SNR margin is 18dB currently, 15dB minimum, 30dB maximum
```



```
 Loop attenuation is 1dB currently, 1dB minimum, 1dB maximum
Current 15-minute performance statistics (115 seconds elapsed):
   0 code violations, 0 loss of sync word seconds
   0 errored seconds, 0 severely errored seconds
   0 unavailable seconds
Packet Statistics:
   0 packets input, 0 bytes, 0 no buffer
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame
   0 abort, 0 ignored, 0 overruns
   32 packets output, 0 bytes, 0 underruns
   0 input clock glitches, 0 output clock glitches
```

*If the user has configured a **Bc** and **Be** value on the virtual circuit, the bandwidth (**BW**) displayed is the sum of those values (Bc + Be). If not, the value for **BW** is the speed of the interface. The **Average utilization** displayed is the average utilization of the displayed bandwidth. If the bandwidth number is the Bc + Be value, the (**limited**) text appears (as shown above).*

show interfaces adsl <*slot/port*>

Use the **show interfaces adsl** command to display information related to the asymmetric digital subscriber line (ADSL) port. Variations of this command include:

show interfaces adsl <*slot/port*>
show interfaces adsl <*slot/port*> **information**
show interfaces adsl <*slot/port*> **information atuc**
show interfaces adsl <*slot/port*> **information atur**
show interfaces adsl <*slot/port*> **information bit-allocation**
show interfaces adsl <*slot/port*> **performance-statistics**
show interfaces adsl <*slot/port*> **performance-statistics** <*x-y*>
show interfaces adsl <*slot/port*> **performance-statistics total-24-hour**
show interfaces adsl <*slot/port*> **performance-statistics total-previous-24-hour**
show interfaces adsl <*slot/port*> **version**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*slot/port*>	Specifies ADSL interface slot and port number.
information	Optional. Displays all ADSL interface information.
atuc	Optional. Displays only ADSL remote information.
atur	Optional. Displays only ADSL local information.
bit-allocation	Optional. Displays only ADSL DMT bit-allocation table.
performance-statistics	Optional. Displays all 96 stored intervals.
<*x-y*>	Optional. Displays only a specified interval (x) or range of intervals (x-y). Valid range is **1** to **96**.
total-24-hour	Optional. Displays only the current 24-hour totals.
total-previous-24-hour	Optional. Displays only the previous 24-hour totals.
version	Optional. Displays current version information (e.g., model and list number, software version, etc.) for the interface.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output for this command:

```
>enable
#show interfaces adsl 1/1 information
adsl 1/1 line information
adsl 1/1 Local Line Information
 Vendor Id:                    00000000
 Serial Number:                00000000
 Firmware Version:
 ADSL Capabilities             G.DMT, G.LITE, ADSL2, ADSL2+
adsl 0/1 Remote Line Information
 Vendor Id:                    00000000
 Serial Number:                00000000
 Firmware Version:             0
 ADSL Capabilities       G.DMT, G.LITE, ADSL2, ADSL2+
```

show interfaces cellular

Use the **show interfaces cellular** command to display configuration parameters and current statistics for a cellular interface. Variations of this command include the following:

show interfaces cellular <*slot*/*port*>
show interfaces cellular <*slot*/*port*> **hardware**
show interfaces cellular <*slot*/*port*> **profile**
show interfaces cellular <*slot*/*port*> **realtime**
show interfaces cellular <*slot*/*port*> **version**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*slot/port*>	Specifies cellular interface slot and port number.
hardware	Optional. Specifies cellular hardware information is displayed.
profile	Optional. Specifies cellular profile information is displayed.
realtime	Optional. Specifies display output is shown in real time.
version	Optional. Specifies cellular version information is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example displays cellular **hardware** information for cellular interface **1/1**:

```
>enable
#show interfaces cellular 1/1 hardware
Electronic Serial Number (ESN) : 0x12345678
Preferred Roaming List (PRL) Version : 12345
Mobile Directory Number (MDN) : 0123456789
Mobile Station ID (MSID) : 0123456789
System ID (SID) : 1234
Network ID (NID) : 12
```


show interfaces dot11ap

Use the **show interfaces dot11ap** command to display information related to a wireless access point (AP), radio, or virtual access point (VAP) interface. Variations of this command include:

show interfaces dot11ap [*<ap>* | *<ap/radio>* | *<ap/radio.vap>***]**
show interfaces dot11ap *<ap>* **control-protocol**
show interfaces dot11ap [*<ap/radio>* | *<ap/radio.vap>***] dot11**

> NOTE
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<ap>	Specifies the AP. Range is **1** to **8**.
</radio>	Specifies the radio associated with the AP. Range is **1** to **2**.
<.vap>	Specifies the VAP associated with the radio. Range is **1** to **8**.
control-protocol	Optional. Displays properties of the control protocol for the AP.
dot11	Optional. Displays counters of an 802.11 radio's VAPs.

> NOTE
> *The radio must be specified in the format <ap/radio> (for example, **2/1** indicates radio 1 on access point 2). The virtual access point must be specified in the format <ap/radio.vap> (for example, **2/1.1** indicates virtual access point 1 on radio 1 on access point 2).*

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output for the AP interface 1 using the **show interfaces dot11ap** command:

```
>enable
#show interfaces dot11ap 1
Dot11 AP 1 line protocol is UP
 Controller Status: Local AC in control
 Ap Version: FW: 1.0 0.4, DRVR: 1.0 0.0, HW: 1.0 0.0
 Ap S/N: LBADTN0625XC975
 AP MAC address: 00:A0:C8:1D:F8:57
 Radio1 - 802.11bg - Enabled, channel 0, address: 00:A0:C8:1D:F8:59
 Radio2 - 802.11a - Disabled, channel 0, address: 00:A0:C8:1D:F8:58
 Bootup Status: Normal
 Ap Status: With Session
 Controlling AC: 00:A0:C8:20:E7:D6
 802.1Q Encapsulation - Disabled
 Auto 100Mbps, Full Duplex

 Ethernet Statistics:
   Ethernet Rx Packets: 291476
   Ethernet Rx Bytes: 20908434
   Ethernet Tx Packets: 67346
   Ethernet Tx Bytes: 10606783
```

The following is sample output for the AP interface 1 using the **show interfaces dot11ap** <*ap*> **control-protocol** command:

```
>enable
#show interfaces dot11ap 1 control-protocol
AP State: Running with session
 Control State: Controlled by this AC
   Control Protocol Transmit Bytes: 4080386
   Control Protocol Receive Bytes: 9435172
   Control Protocol Transmit Packets: 52203
   Control Protocol Receive Packets: 65931
   Control Protocol Receive Keepalives: 14914
   Control Protocol Receive Security Errors: 0
   Control Protocol Dropped Packets: 0
   Control Protocol Protocol Errors: 0
   Control Protocol Protocol No Responses: 0
```


The following is sample output for the radio interface 1 on AP interface 1 using the **show interfaces dot11ap** <*ap/radio*> *dot11* command:

```
>enable
#show interfaces dot11ap 1/1 dot11
Authentication Count: 17
 Deauthentication Count: 48
 Association Count: 18
 Disassociation Count: 12
 Reassociation Count: 0
 Wireless MSDU Rx Packets: 346
 Wireless Data Rx Packets: 7221
 Wireless Multicast Rx Packets: 308
 Wireless Management Rx Packets: 667521
 Wireless Control Rx Packets: 0
 Wireless MSDU Tx Packets: 236613
 Wireless Data Tx Packets: 236210
 Wireless Multicast Tx Packets: 236166
 Wireless Management Tx Packets: 599
 Wireless Control Tx Packets: 0
```


show interfaces efm-group

Use the **show interfaces efm-group** command to view the interface statistics for the specified Ethernet in the first mile (EFM) group. Variations of this command include:

show interfaces efm-group all
show interfaces efm-group all connections
show interfaces efm-group *<group number>*
show interfaces efm-group *<group number>* **connections interval 15-minute** *<value>*
show interfaces efm-group *<group number>* **connections interval 24-hour** *<value>*
show interfaces efm-group *<group number>* **interval 15-minute** *<value>*
show interfaces efm-group *<group number>* **interval 24-hour** *<value>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

all	Displays statistics for all EFM groups.
<group number>	Displays statistics for a single EFM group. Range is **1** to **1024**.
connections	Optional. Displays the statistics for the connected interfaces.
interval 15-minute	Optional. Displays the statistics for a 15-minute period in the last 24 hours.
interval 24-hour	Optional. Displays the statistics for a 24-hour period in the last 7 days.
<value>	Specifies which 15-minute period in the last 24 hours or which 24-hour period in the last 7 days is displayed. Range for 15-minute periods is **1** to **4**; range for 24-hour periods is **1** to **7**.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example shows the statistics for the interfaces connected to EFM group **1** in the first 15-minute period of the last 24 hours:

```
>enable
#show interfaces efm-group 1 connections interval 15-minute 1
EFM Group 1 Connections (15-Minute Interval 1):
    412/900 seconds elapsed in interval
    interface shdsl 1/1 connected
            NE in sync, FE in sync,
            NE in tx, FE in tx
            No alarms.
            109 fragments input, 1111 fragments output
            0 errored fragments, 0 discarded fragments
            0 fragments too small, 0 fragments too large
            0 fcs errors, 0 coding errors
    interface shdsl 1/2 connected
            NE in sync, FE in sync,
            NE in tx, FE in tx
            No alarms.
            109 fragments input, 1111 fragments output
            0 errored fragments, 0 discarded fragments
            0 fcs errors, 0 coding errors
    interface shdsl 1/3 connected
            NE in sync, FE in sync,
            NE in tx, FE in tx
            No alarms.
            109 fragments input, 1121 fragments output
            0 errored fragments, 0 discarded fragments
            0 fcs errors, 0 coding errors
    interface shdsl 1/4 connected
            NE in sync, FE in sync,
            NE in tx, FE in tx
            No alarms.
            109 fragments input, 1109 fragments output
            0 errored fragments, 0 discarded fragments
            0 fcs errors, 0 coding errors
```

show interfaces gigabit-switchport <*slot/port*>

Use the **show interfaces gigabit-switchport** command to display configuration parameters and current statistics for gigabit switchport interfaces. These commands are valid only on AOS units with gigabit switchport interfaces. Variations of this command include the following:

show interfaces gigabit-switchport <*slot/port*>
show interfaces gigabit-switchport <*slot/port*> **realtime**
show interfaces gigabit-switchport <*slot/port*> **switchport**
show interfaces gigabit-switchport <*slot/port*> **switchport vlans**

*Not all subcommands apply to all interfaces or are available on all AOS units. Type **show interfaces** <interface> **?** for a list of valid subcommands for the specified interface. Some subcommands are only valid on AOS units with switchport or gigabit switchport interfaces. Enter the **show interfaces ?** command to display a list of valid subcommands for your specific platform.*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*slot/port*>	Specifies a gigabit switchport interface slot and port number. Type **show interfaces description** for a complete list of valid gigabit switchport interfaces.
switchport	Displays switchport settings and statistics for the specified gigabit switchport interface.
vlans	Optional. Displays the VLAN membership information for a specific gigabit switchport interface.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show interfaces gigabit-switchport 0/1** command:

```
>enable
#show interfaces gigabit-switchport 0/1
giga-swx 0/1 is UP, line protocol is UP
  Hardware address is 00:A0:C8:01:2F:55
  RJ-45 Shielded
  100Mb/s, negotiated full-duplex, configured full-duplex
  input flow control is disabled, 0 pause frames received
  ARP type: ARPA; ARP timeout is 20 minutes
  Last clearing of "show interface" counters: never
  5 minute input rate 6128 bits/sec, 7 packets/sec
  5 minute output rate 640 bits/sec, 1 packets/sec
    0 total jumbo frames
    41005094 packets input, 3524287214 bytes
    20102647 unicasts, 15808395 broadcasts, 5094052 multicasts input
    0 unknown protocol, 9830 discards
    0 input errors, 0 runts, 0 giants
    0 alignment errors, 0 crc errors
    236869 packets output, 71234821 bytes
    75670 unicasts, 57387 broadcasts, 103812 multicasts output
    0 output errors, 0 deferred, 0 discards
    0 single, 0 multiple, 0 late collisions
    0 excessive collisions

  L3 Switch
    498 packets input, 0 packets forwarded
    0 header errors, 11 discards
```

The following is sample output from the **show interfaces gigabit-switchport 0/1 switchport** command:

```
>enable
#show interfaces gigabit-switchport 0/1 switchport
Name: giga-swx 0/1
Switchport: enabled
Administrative Mode: access
Negotiation of Trunking: access
```


Access Mode VLAN (configured): 1
Trunking Native Mode VLAN: 1
Trunking VLAN Enabled: 1-4094
Trunking VLAN GVRP Fixed: none
Port Expiration: disabled
Port Security: disabled
Protected: false

The following is sample output from the **show interfaces gigabit-switchport 0/1 switchport vlan** command:

>**enable**
#show interfaces gigabit-switchport 0/1 switchport vlan
Interface Membership Vlans
---
giga-swx 0/1 Configured 1

show interfaces shdsl <*slot/port*> splice-detect

Use the **show interfaces shdsl splice-detect** command to view the bad splice detection test results for the specified interface. Variations of this command include:

show interfaces shdsl <*slot/port*> **splice-detect 24-hour**

show interfaces shdsl <*slot/port*> **splice-detect 24-hour** <*interval*>

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*slot/port*>	Specifies the slot and port of the interface on which the test was run.
splice-detect 24-hour	Displays the bad splice detection test results for the last 24 hours.
<*interval*>	Optional. Specifies that results from one or more of the previous 24-hour intervals are displayed. Valid interval range is **1** to **7**. You can enter a single interval, or a range of intervals when separated by a dash.

Default Values

No default values are necessary for this command.

Command History

Release A4.05	Command was introduced.

Usage Examples

The following example displays the bad splice detection test results for SHDSL interface **1/1** over the past 24 hours:

#show interfaces shdsl 1/1 splice-detect 24-hour

Current Splice Detect Data

Summary: No Trouble Found

Distance (ft)	Count
0	0
200	0
400	0
600	0
800	0
1000	0
1200	0

show interfaces switchport <*slot/port*>

Use the **show interfaces switchport** command to display configuration parameters and current statistics for switchport interfaces. These commands are valid only on AOS units with switchport interfaces. Variations of this command include the following:

show interfaces switchport <*slot/port*> **realtime**
show interfaces switchport <*slot/port*> **switchport**
show interfaces switchport <*slot/port*> **switchport vlans**

*Not all subcommands apply to all interfaces or are available on all AOS units. Type **show interfaces** <interface> **?** for a list of valid subcommands for the specified interface. Some subcommands are only valid on AOS units with switchport or gigabit switchport interfaces. Enter the **show interfaces ?** command to display a list of valid subcommands for your specific platform.*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<slot/port>	Specifies a switchport interface slot and port number. Type **show interfaces description** for a complete list of valid switchport interfaces.
switchport	Displays switchport settings and statistics for the specified switchport interface.
vlans	Optional. Displays the VLAN membership information for a specific switchport interface.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 10.1	Command was expanded to include the **vlans** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show interfaces switchport 0/1** command:

```
>enable
#show interfaces switchport 0/1
swx 0/1 is DOWN, line protocol is DOWN
  Hardware address is 00:A0:C8:00:61:22
  BW is 10000 Kbit
  ?b/s, negotiated ? duplex, configured full-duplex
  input flow control is disabled, 0 pause frames received
  ARP type: ARPA; ARP timeout is 20 minutes
  Last clearing of "show interface" counters: never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    Queueing method: fifo
    Output queue: 0/256/0 (size/max total/drops)
    Interface Shaper: NOT ENABLED
    0 packets input, 0 bytes
    0 unicasts, 0 broadcasts, 0 multicasts input
    0 symbol errors, 0 discards
    0 input errors, 0 runts, 0 giants
    0 alignment errors, 0 crc errors
    0 packets output, 0 bytes
    0 unicasts, 0 broadcasts, 0 multicasts output
    0 output errors, 0 deferred, 0 discards
    0 single, 0 multiple, 0 late collisions
    0 excessive collisions
```

The following is sample output from the **show interfaces switchport 0/1 switchport** command:

```
>enable
#show interfaces switchport 0/1 switchport
Name: swx 0/1
Switchport: enabled
Administrative Mode: access
Negotiation of Trunking: access
Access Mode VLAN (configured): 1
Trunking Native Mode VLAN: 1
```


Trunking VLAN Enabled: 1-4094
Trunking VLAN GVRP Fixed: none
Port Expiration: disabled
Port Security: disabled

The following is sample output from the **show interfaces switchport 0/1 switchport vlans** command:

>**enable**
#show interfaces switchport 0/1 switchport vlans
Interface Membership Vlans
---
swx 0/1 Configured 1

show ip access-lists

Use the **show ip access-lists** command to display all configured Internet Protocol version 4 (IPv4) access control lists (ACLs) in the system. Variations of this command include:

show ip access-lists
show ip access-lists *<ipv4 acl name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv4 acl name>	Optional. Specifies a particular IPv4 ACL to display.

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

The **show ip access-lists** command displays all configured IPv4 ACLs in the system. All entries in the IPv4 ACL are displayed, and a counter indicating the number of packets matching the entry is listed.

Usage Examples

The following is sample output from the **show ip access-lists** command, and displays information for IPv4 ACLs:

```
>enable
#show ip access-lists
Standard IP access list MatchAll
   permit host 10.3.50.6 (0 matches)
   permit 10.200.5.0 wildcard bits 0.0.0.255 (0 matches)
Extended IP access list UnTrusted
   deny   icmp 10.5.60.0 wildcard bits 0.0.0.255 any source-quench (0 matches)
   deny   tcp any any   (0 matches)
```


show ip arp

Use the **show ip arp** command to display the Address Resolution Protocol (ARP) table. Variations of this command include:

show ip arp
show ip arp realtime
show ip arp vrf <*name*>
show ip arp vrf <*name*> **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance or your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.
vrf <*name*>	Optional. Displays information only for the specified virtual routing and forwarding (VRF).

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **show ip arp** command:

```
>enable
#show ip arp
ADDRESS         TTL(min)    MAC ADDRESS        INTERFACE    TYPE
10.22.18.3      19          00:E0:29:6C:BA:31  eth 0/1      Dynamic
192.168.20.2    16          00:A0:C8:0D:E9:AD  eth 0/2      Dynamic
224.0.0.5       20          01:00:5E:00:00:05  eth 0/2      Permanent
```


show ip cache

Use the **show ip cache** command to display the contents of the Internet Protocol version 4 (IPv4) route cache for each interface in a given virtual private network (VPN) routing and forwarding (VRF) instance. The route cache contains information about which egress interface, IPv4 gateway address, and MAC address to use when forwarding packets to a given destination. Variations of this command include:

show ip cache
show ip cache vrf <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

vrf <*name*>	Optional. Specifies a nondefault VRF instance for which to display route cache information. If no VRF instance is specified, route cache information for the default VRF instance is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **show ip cache** command for the default VRF (router):

```
>enable
#show ip cache
DESTINATION     INTERFACE  NEXT HOP      USE COUNT  MAC ADDRESS
224.0.0.5       Loopback   127.0.0.1     0
10.22.18.3      eth 0/1    10.22.18.3    0          00:E0:29:6C:BA:31
10.22.18.6      Loopback   127.0.0.1     18
192.168.30.2    eth 0/2    192.168.20.2  0          00:A0:C8:0D:E9:AD
10.22.18.255    Loopback   127.0.0.1     2
255.255.255.255 Loopback   127.0.0.1     2
192.168.20.1    Loopback   127.0.0.1     25
IP routing cache 7 entries
```

show ip crypto ipsec

Use the **show ip crypto ipsec** command to display information regarding the Internet Protocol security (IPsec) configuration. Variations of this command include the following:

show ip crypto ipsec sa
show ip crypto ipsec sa address *<ip address>*
show ip crypto ipsec sa brief
show ip crypto ipsec sa ffe-id *<rapidroute interface ID>*
show ip crypto ipsec sa map *<name>*
show ip crypto ipsec sa profile *<name>*
show ip crypto ipsec sa remote-id *<name>*
show ip crypto ipsec timeline
show ip crypto ipsec transform-set
show ip crypto ipsec transform-set *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

sa	Displays all IPsec security associations (SAs).
sa address *<ip address>*	Optional. Displays all IPsec SAs associated with the designated peer IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
sa brief	Optional. Displays a brief listing of IPsec SAs.
sa ffe-id *<rapidroute interface ID>*	Optional. Displays all IPsec SAs associated with a specific RapidRoute interface. RapidRoute interfaces have a numerical identifier that ranges between **1** and **16777215**. These identifiers are displayed in the various outputs of the **show ip ffe** commands beginning with the command *show ip ffe on page 708***.**
sa map *<name>*	Optional. Displays all IPsec SAs associated with the specified crypto map.
sa profile *<name>*	Optional. Displays all IPsec SAs associated with the specified IPsec profile.
sa remote-id	Optional. Displays all IPsec SAs associated with the designated peer remote ID.
timeline	Optional. Displays a timeline of VPN tunnel creation and peak number of tunnels per hour.

transform-set	Displays all defined transform sets.
<name>	Optional. Displays information for a specific transform set.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 15.1	Command was expanded to include the **brief** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.6	Command was expanded to include the **ffe-id** parameter.
Release A4.01	Command was expanded to include the **timeline** parameter.
Release R10.5.0	Command syntax was changed to require the **ip** parameter.
Release R11.9.0	Command was expanded to include the **sa profile** <*name*> parameter.

Usage Examples

The following is sample output from the **show ip crypto ipsec sa** command:

>**enable**
#show ip crypto ipsec sa
Using 2 SAs out of 4000
Peak concurrent SAs: 2
IPsec Security Associations:

Peer IP Address: 3.3.3.1
  Remote ID: 3.3.3.2
  Crypto Map: VPN 10
  Direction: Inbound
  Encapsulation: ESP
  SPI: 0xF38B37A1 (4085987233)
  FFE ID: 1
  RX Bytes: 281728
  Selectors: Src:10.0.2.0/255.255.255.0 Port:ANY Proto:ALL IP
        Dst:10.0.1.0/255.255.255.0 Port:ANY Proto:ALL IP
  Hard Lifetime: 28570
  Soft Lifetime: 0
  Out-of-Sequence Errors: 0

show ip crypto map

Use the **show ip crypto map** command to display information regarding Internet Protocol version 4 (IPv4) crypto map settings. Variations of this command include the following:

show ip crypto map
show ip crypto map interface *<interface>*
show ip crypto map *<name>*
show ip crypto map *<name> <number>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interface *<interface>*	Optional. Displays the IPv4 crypto map settings for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show crypto map interface ?** for a complete list of valid interfaces.
<name>	Optional. Specifies an IPv4 specific crypto map name.
<number>	Optional. Specifies an IPv4 specific crypto map number.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.7.0	Command was changed to include the **ip** keyword for Internet Protocol version 6 (IPv6) support.

Usage Examples

The following is sample output from the **show ip crypto map** command:

```
>enable
#show ip crypto map testMap
Crypto Map “testMap” 10 ipsec-ike
 Extended IP access list NewList
 Peers:
   63.97.45.57
 Transform sets:
   esp-des
 Security-association lifetimes:
   0 kilobytes
   86400 seconds
 No PFS group configured
 Interfaces using crypto map testMap:
   eth 0/1
```


show ip dhcp binding

Use the **show ip dhcp binding** command to display the Dynamic Host Client Protocol version 4 (DHCPv4) server client table with associated information. Variations of this command include:

show ip dhcp binding
show ip dhcp binding *<ipv4 address>*
show ip dhcp binding vrf *<name>*
show ip dhcp binding vrf *<name> <ipv4 address>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv4 address>	Optional. Specifies the IPv4 address of the specified client. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrf *<name>*	Optional. Displays information only for the specified virtual routing and forwarding (VRF) instance. If a VRF is not specified, the default VRF is assumed.

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.
Release 17.1	Command was expanded to include the **vrf** parameter and the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command syntax was changed to remove the hyphen and the **server** keyword on Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **server** keyword on Adtran voice products.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **show ip dhcp binding** command:

```
>enable
#show ip dhcp binding
IP Address      Client Id              Lease Expiration        Client Name
10.100.23.64    01:00:a0:c8:00:8f:b3   Aug 15 2002 11:02 AM    Router
```

The following is sample output from the **show ip dhcp binding vrf Gray** command:

```
>enable
#show ip dhcp binding vrf Gray
IP Address      Client Id              Lease Expiration        Client Name
192.168.19.2    01:00:e0:29:91:1e:27   Oct 16 2007 10:58 AM    Estclair4
192.168.19.3    01:00:e0:81:01:53:01   Oct 16 2007 12:42 PM    sylvester
192.168.19.4    01:00:15:c5:6a:69:ec   Oct 16 2007 1:35 PM     Dell-Wifi06
```

show ip dhcp lease

Use the **show ip dhcp lease** command to display all Dynamic Host Client Protocol version 4 (DHCPv4) lease information for interfaces that have dynamically assigned IPv4 addresses. Variations of this command include:

show ip dhcp lease
show ip dhcp lease *<interface>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Optional. Displays the information for the specified interface type. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show ip dhcp lease ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release 18.3	Command syntax was changed to remove the hyphen and the **client** keyword for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **client** keyword for Adtran voice products.
Release R11.7.0	Command was expanded to include the Ethernet in the first mile (EFM) group interface.

Usage Examples

The following is sample output from the **show ip dhcp lease** command:

```
>enable
#show ip dhcp lease
Interface: ethernet 0/1
Temp IP address: 10.100.23.64 Mask: 0.0.0.0
   DHCP Lease server: 10.100.23.207 State: Bound (3)
   Lease: 120 seconds
Temp default gateway address: 0.0.0.0
   Client-ID: N/A
```

show ip ffe

Use the **show ip ffe** command to display current Internet Protocol version 4 (IPv4) RapidRoute fast forwarding engine (FFE) entries. Variations of this command include:

show ip ffe

show ip ffe destination <*ipv4 address*>
show ip ffe destination <*ipv4 address*> **egress** <*interface*>
show ip ffe destination <*ipv4 address*> **egress ipsec** <*rapidroute interface ID*>
show ip ffe destination <*ipv4 address*> **egress system-control-evc**
show ip ffe destination <*ipv4 address*> **egress system-management-evc**

show ip ffe destination <*ipv4 address*> **ingress** <*interface*>
show ip ffe destination <*ipv4 address*> **ingress ipsec** <*rapidroute interface ID*>
show ip ffe destination <*ipv4 address*> **ingress system-control-evc**
show ip ffe destination <*ipv4 address*> **ingress system-management-evc**

show ip ffe destination-port <*port*>
show ip ffe destination-port <*port*> **egress** <*interface*>
show ip ffe destination-port <*port*> **egress ipsec** <*rapidroute interface ID*>
show ip ffe destination-port <*port*> **egress system-control-evc**
show ip ffe destination-port <*port*> **egress system-management-evc**

show ip ffe destination-port <*port*> **ingress** <*interface*>
show ip ffe destination-port <*port*> **ingress ipsec** <*rapidroute interface ID*>
show ip ffe destination-port <*port*> **ingress system-control-evc**
show ip ffe destination-port <*port*> **ingress system-management-evc**

show ip ffe details
show ip ffe details egress <*interface*>
show ip ffe details egress ipsec <*rapidroute interface ID*>
show ip ffe details egress system-control-evc
show ip ffe details egress system-management-evc

show ip ffe details ingress <*interface*>
show ip ffe details ingress ipsec <*rapidroute interface ID*>
show ip ffe details ingress system-control-evc
show ip ffe details ingress system-management-evc

show ip ffe egress <*interface*>
show ip ffe egress <*interface*> **destination** <*ipv4 address*>
show ip ffe egress <*interface*> **destination-port** <*port*>
show ip ffe egress <*interface*> **details**
show ip ffe egress <*interface*> **icmp-type** <*type*>
show ip ffe egress <*interface*> **protocol** <*protocol*>

show ip ffe egress <*interface*> **source** <*ipv4 address*>
show ip ffe egress <*interface*> **source-port** <*port*>
show ip ffe egress <*interface*> **type** <*type*>
show ip ffe egress ipsec <*rapidroute interface ID*>

show ip ffe egress system-control-evc destination <*ipv4 address*>
show ip ffe egress system-control-evc destination-port <*port*>
show ip ffe egress system-control-evc details
show ip ffe egress system-control-evc icmp-type <*type*>
show ip ffe egress system-control-evc protocol <*protocol*>
show ip ffe egress system-control-evc source <*ipv4 address*>
show ip ffe egress system-control-evc source-port <*port*>
show ip ffe egress system-control-evc type <*type*>

show ip ffe egress system-management-evc destination <*ipv4 address*>
show ip ffe egress system-management-evc destination-port <*port*>
show ip ffe egress system-management-evc details
show ip ffe egress system-management-evc icmp-type <*type*>
show ip ffe egress system-management-evc protocol <*protocol*>
show ip ffe egress system-management-evc source <*ipv4 address*>
show ip ffe egress system-management-evc source-port <*port*>
show ip ffe egress system-management-evc type <*type*>

show ip ffe icmp-type <*type*>
show ip ffe icmp-type <*type*> **egress** <*interface*>
show ip ffe icmp-type <*type*> **egress** <*interface*> **system-control-evc**
show ip ffe icmp-type <*type*> **egress** <*interface*> **system-management-evc**

show ip ffe icmp-type <*type*> **ingress** <*interface*>
show ip ffe icmp-type <*type*> **ingress** <*interface*> **system-control-evc**
show ip ffe icmp-type <*type*> **ingress** <*interface*> **system-management-evc**
show ip ffe icmp-type <*type*> **ipsec** <*rapidroute interface ID*>

show ip ffe ingress <*interface*>
show ip ffe ingress <*interface*> **destination** <*ipv4 address*>
show ip ffe ingress <*interface*> **destination-port** <*port*>
show ip ffe ingress <*interface*> **details**
show ip ffe ingress <*interface*> **icmp-type** <*type*>
show ip ffe ingress <*interface*> **protocol** <*protocol*>
show ip ffe ingress <*interface*> **source** <*ipv4 address*>
show ip ffe ingress <*interface*> **source-port** <*port*>
show ip ffe ingress <*interface*> **type** <*type*>
show ip ffe ingress ipsec <*rapidroute interface ID*>

show ip ffe ingress system-control-evc destination <*ipv4 address*>
show ip ffe ingress system-control-evc destination-port <*port*>

show ip ffe ingress system-control-evc details
show ip ffe ingress system-control-evc icmp-type <*type*>
show ip ffe ingress system-control-evc protocol <*protocol*>
show ip ffe ingress system-control-evc source <*ipv4 address*>
show ip ffe ingress system-control-evc source-port <*port*>
show ip ffe ingress system-control-evc type <*type*>

show ip ffe ingress system-management-evc destination <*ipv4 address*>
show ip ffe ingress system-management-evc destination-port <*port*>
show ip ffe ingress system-management-evc details
show ip ffe ingress system-management-evc icmp-type <*type*>
show ip ffe ingress system-management-evc protocol <*protocol*>
show ip ffe ingress system-management-evc source <*ipv4 address*>
show ip ffe ingress system-management-evc source-port <*port*>
show ip ffe ingress system-management-evc type <*type*>

show ip ffe peak
show ip ffe peak history

show ip ffe protocol <*protocol*>
show ip ffe protocol <*protocol*> **egress** <*interface*>
show ip ffe protocol <*protocol*> **egress system-control-evc**
show ip ffe protocol <*protocol*> **egress system-management-evc**

show ip ffe protocol <*protocol*> **ingress** <*interface*>
show ip ffe protocol <*protocol*> **ingress system-control-evc**
show ip ffe protocol <*protocol*> **ingress system-management-evc**
show ip ffe protocol <*protocol*> **ipsec** <*rapidroute interface ID*>

show ip ffe source <*ipv4 address*>
show ip ffe source <*ipv4 address*> **egress** <*interface*>
show ip ffe source <*ipv4 address*> **egress system-control-evc**
show ip ffe source <*ipv4 address*> **egress system-management-evc**
show ip ffe source <*ipv4 address*> **egress** <*interface*> **ipsec** <*rapidroute interface ID*>

show ip ffe source <*ipv4 address*> **ingress** <*interface*>
show ip ffe source <*ipv4 address*> **ingress system-control-evc**
show ip ffe source <*ipv4 address*> **ingress system-management-evc**
show ip ffe source <*ipv4 address*> **ingress** <*interface*> **ipsec** <*rapidroute interface ID*>

show ip ffe source-port <*port*>
show ip ffe source-port <*port*> **egress** <*interface*>
show ip ffe source-port <*port*> **egress system-control-evc**
show ip ffe source-port <*port*> **egress system-management-evc**
show ip ffe source-port <*port*> **egress** <*interface*> **ipsec** <*rapidroute interface ID*>

show ip ffe source-port <*port*> **ingress** <*interface*>
show ip ffe source-port <*port*> **ingress system-control-evc**
show ip ffe source-port <*port*> **ingress system-management-evc**
show ip ffe source-port <*port*> **ingress** <*interface*> **ipsec** <*rapidroute interface ID*>

show ip ffe type <*type*>
show ip ffe type <*type*> **egress** <*interface*>
show ip ffe type <*type*> **egress system-control-evc**
show ip ffe type <*type*> **egress system-management-evc**
show ip ffe type <*type*> **egress** <*interface*> **ipsec** <*rapidroute interface ID*>

show ip ffe type <*type*> **ingress** <*interface*>
show ip ffe type <*type*> **ingress system-control-evc**
show ip ffe type <*type*> **ingress system-management-evc**
show ip ffe type <*type*> **ingress** <*interface*> **ipsec** <*rapidroute interface ID*>

show ip ffe wildcard
show ip ffe wildcard interface <*interface*>
show ip ffe wildcard system-control-evc
show ip ffe wildcard system-management-evc

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

destination <*ipv4 address*>	Optional. Filters output by a destination IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
destination-port <*port*>	Optional. Filters output by destination Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port. Ports range from **0** to **65535**.
details	Optional. Displays detailed information. Refer to the Functional Notes for more information about using the **details** keyword.

egress <*interface*> Optional. Displays RapidRoute entries for an egress interface. Specify an interface in the format <*interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | group id]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an EFM group interface, use **efm-group 1**. Type **show ip ffe egress ?** to display a complete list of valid interfaces.

egress ipsec <*rapidroute interface ID*> Optional. Displays RapidRoute entries that come from an Internet Protocol security (IPsec) security association (SA) on a specified RapidRoute interface. RapidRoute interface identifiers range from **1** to **16777215**.

icmp-type <*type*> Optional. Displays RapidRoute entries using a specific Internet Control Message Protocol (ICMP) type. There are three types of ICMP to choose from:

- **echo** Displays ICMP echo RapidRoute entries.
- **reply** Displays ICMP reply RapidRoute entries.
- **0** to **255** Displays other ICMP types.

ingress <*interface*> Optional. Displays RapidRoute entries for an ingress interface. Specify an interface in the format <*interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | group id]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an EFM group interface, use **efm-group 1**. Type **show ip ffe ingress ?** to display a complete list of valid interfaces.

ingress ipsec <*rapidroute interface ID*> Optional. Displays RapidRoute entries that go to an IPsec SA on a specified RapidRoute interface. RapidRoute interface identifiers range from **1** to **16777215**.

peak Optional. Displays the current and peak count of RapidRoute sessions. Information is displayed for each eligible interface and the global values.

history Optional. Displays a graphical presentation of the peak global RapidRoute cont per second for the last 60 seconds. Additionally displays the peak and average global RapidRoute count per minute for the last 60 minutes, as well as the peak and average global RapidRoute count per hour for the last 72 hours.

protocol <*protocol*> Optional. Displays RapidRoute entries that use a specified protocol. Protocols can be specified by selecting one of the following:

- **ah** Displays Authentication Header (AH) Protocol RapidRoute entries.
- **esp** Displays Encapsulating Security Payload (ESP)

		Protocol RapidRoute entries.
	fragment	Displays fragmented (FRAG) RapidRoute entries.
	gre	Displays Generic Route Encapsulation (GRE) Protocol RapidRoute entries.
	icmp	Displays ICMP RapidRoute entries.
	tcp	Displays TCP RapidRoute entries.
	udp	Displays UDP RapidRoute entries.
	0 to **255**	Displays other protocol types.
source <*ipv4 address*>		Optional. Displays RapidRoute entries for a specified source IPv4 address. IPv4 addresses should be expressed in decimal dotted notation (for example, **10.10.10.1**).
source-port <*port*>		Optional. Displays RapidRoute entries for a specified TCP or UDP source port. Ports range from **0** to **65535**.
system-control-evc		Optional. Displays RapidRoute entries for the system control Ethernet virtual connection (EVC).
system-management-evc		Optional. Displays RapidRoute entries for the system management EVC.
type <*type*>		Optional. Displays RapidRoute entries of a specific type. Specified types include one of the following:
	ineligible	Displays only ineligible RapidRoute entries.
	rejected	Displays only rejected RapidRoute entries.
	valid	Displays only valid RapidRoute entries.
wildcard		Optional. Displays wildcards for each IP interface.
interface <*interface*>		Optional. Limits the output to the specified interface. Interfaces are specified in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | group id]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an EFM group interface, use **efm-group 1**. Type **show ip ffe wildcard interface ?** to display a complete list of valid interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.6	Command was expanded to include the **ipsec** and **gre** parameters.

Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.5.0	Command was expanded so that the **ipsec** parameter can be used to filter the command output.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R11.2.0	Command was expanded to include high level data link control (HDLC) interface.
Release R11.3.0	Command was expanded to include the Ethernet in the first mile (EFM) group interface.
Release R11.4.0	Command was expanded to include the **fragment** option for the **protocol** parameter.
Release R11.10.0	Command was expanded to include the **peak** and **wildcard** parameters.
Release R13.7.0	Command was expanded to include the virtual local area network (VLAN) interface.

Functional Notes

The **show ip ffe** command can be further filtered by adding any combination of the following parameters:

destination <*ipv4 address*>
destination-port <*port*>
details
egress <*interface*>
egress ipsec <*rapidroute interface ID*>
icmp-type <*type*>
ingress <*interface*>
ingress ipsec <*rapidroute interface ID*>
ipsec <*rapidroute interface ID*>
protocol <*protocol*>
source <*ipv4 address*>
source-port <*port*>
type <*type*>

For example, the **destination** <*ipv4 address*> and **source** <*ipv4 address*> parameters can be used in conjunction with one another. In this case, the command would look like as follows:

#show ip ffe destination 10.10.10.3 source 10.10.10.1

These parameters can be combined in any order and as many times as is necessary to get the desired output.

*The **detail** keyword must be the last keyword in the command. For example, **show ip ffe destination** <ipv4 address> **egress** <interface> **source-port** <port> **details** is acceptable, but **show ip ffe destination** <ipv4 address> **details egress** <interface> is not.*

Data for the **peak history** parameters is presented as a percentage of the value configured with the command *ip ffe max-entries <value> on page 1364*. Changing the **ip ffe max-entries** value clears the related FFE peak information.

Usage Examples

The following is sample output from the **show ip ffe** command:

```
>enable
#show ip ffe
Timeout     TCP     UDP     ICMP    AH      ESP     GRE     Other
Age:        30m0s   30m0s   30m0s   30m0s   30m0s   30m0s   30m0s
Inactive:   15s     15s     15s     15s     15s     15s     15s
Type:  * valid, ! ineligible, - rejected
Flags: F firewall, N NAT, T altered ToS, D don't fragment, I IPsec
--------------------------------
Ingress: eth 0/1
   149 hits, 62553 misses, 0 drops
T   Proto Source           Destination      Specific      Age   Used  Drops  Flags
!   udp   10.200.2.7       10.200.205.255   3959          137   17s   10     0
!   udp   10.200.201.170   10.200.255.255   138           138   16s   0      0
!   udp   10.200.7.200     10.200.255.255   138           138   16s   0      0
!   udp   10.200.201.198   10.200.255.255   138           138   4s    0      0
!   udp   10.200.201.198   10.200.255.255   137           137   7s    2      0
!   tcp   172.22.77.208    10.200.1.134     2668          23    6s    36     0
Number of entries: 6 of 6 (4096 maximum)
--------------------------------
Total number of entries: 6 of 6 (16384 maximum)
```

The following is sample output from the **show ip ffe details** command:

```
Timeout     TCP     UDP     ICMP    AH      ESP     GRE     Other
Age:        30m0s   30m0s   30m0s   30m0s   30m0s   30m0s   30m0s
Inactive:   15s     15s     15s     15s     15s     15s     15s
Type:  * valid, ! ineligible, - rejected
Flags: F firewall, N NAT, T altered ToS, D don't fragment, I IPsec
--------------------------------
Ingress: eth 0/1
   706189 hits, 45 misses, 0 drops
T Proto Source        Destination     Specific      Age   Used Drops Flags
* icmp  10.0.1.2      10.0.2.2        echo     13   13s   129  0     I
   egress: Outbound ESP SA 2
Number of entries: 1 of 1  (4096 maximum)
--------------------------------
Ingress: Inbound ESP SA 1
   129 hits, 1 misses, 0 drops
```



```
T Proto Source        Destination     Specific       Age   Used Drops Flags
* icmp  10.0.2.2      10.0.1.2        reply    13    13s   129    0    I
   egress: eth 0/1 (10.0.1.2)
Number of entries: 1 of 1  (4096 maximum)

--------------------------------
Ingress: Outbound ESP SA 2
   129 hits, 1 misses, 0 drops
T Proto Source        Destination     Specific       Age   Used   Drops   Flags
* esp   3.3.3.1       3.3.3.2         0x923dbab4     13s   129    0       I
   egress: hdlc 1
Number of entries: 1 of 1  (256 maximum)
--------------------------------

Total number of entries: 3 of 3  (16384 maximum)
```

The following is sample output from the **show ip ffe** command when wildcards are in use; any field that has been wildcarded appears as **any**:

```
Timeout     TCP      UDP      ICMP     AH       ESP      GRE      Other
Age:        30m0s    30m0s    30m0s    30m0s    30m0s    30m0s    30m0s
Inactive:   15s      15s      15s      15s      15s      15s      15s

Exceptions: 0/217/0 (current/max/drops)

Type:  * valid, ! ineligible, - rejected
Flags: F firewall, N NAT, T altered ToS, D don't fragment, I IPsec, H hardware assist, i ingress filter,
       e egress filter
--------------------------------
Ingress: system-management-evc
   0 hits, 27660 misses, 1 drops
T    Proto   ToS      Age      Used   Drops   Flags   Source          Destination
!    any      any     4m12s    38     0               any             10.17.152.255
!    any      any     3s       29     0               any             10.17.152.31
Number of entries: 2 of 2 (4096 maximum)
```

The following is sample output from the **show ip ffe wildcard** command:

```
>enable
#show ip ffe wildcard
Field                          Wildcarded
============================   ============================
eth 0/1
    Source IP Address          :No
    Dest IP Address            :No (always)
    IP Precedence              :No
    IP DSCP                    :Yes
    IP Protocol (L4)           :Yes
    TCP Source Port            :Yes
    TCP Destination Port       :Yes
    UDP Source Port            :Yes
    UDP Destination Port       :Yes
    ICMP Type, Code and ID     :Yes
    ESP SPI                    :Yes
    GRE Tunnel Key             :Yes

eth 0/2
    Source IP Address          :Yes
    Dest IP Address            :No (always)
    IP Precedence              :Yes
    IP DSCP                    :Yes
    IP Protocol (L4)           :Yes
    TCP Source Port            :Yes
    TCP Destination Port       :Yes
    UDP Source Port            :Yes
    UDP Destination Port       :Yes
    ICMP Type, Code and ID     :Yes
    ESP SPI                    :Yes
    GRE Tunnel Key             :Yes
```


show ip ffe summary

Use the **show ip ffe summary** command to display a summary of all the current Internet Protocol version 4 (IPv4) RapidRoute fast forwarding engine (FFE) entries.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip ffe summary** command:

```
>enable
#show ip ffe summary
Ingress    MaxEntries   Entries   Hits   Misses   Drops
eth 0/1    4096         1         0      56       0
global     16384        1         0      56       0
```


show ip flow

Use the **show ip flow** command to display information regarding the configuration of integrated traffic monitoring (ITM) on your AOS product. Variations of this command include:

show ip flow cache
show ip flow export
show ip flow interface

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

cache	Displays a summary of the current state of the cache of nonexpired traffic flows.
export	Displays information on export packets sent to a destination.
interface	Displays the ITM configuration of each interface on the router.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip flow export** command:

#show ip flow export

```
Traffic Flow export is ENABLED
    Version: 9
    Export Destinations
        10.22.16.132: 9991
            vrf BLUE
            source ppp 1
        10.5.22.203: 30000
    11 flows exported in 8 udp datagrams
    0 flows failed to export
```


The following is sample output from the **show ip flow cache** command:

```
#show ip flow cache
IP Traffic Flow Cache
    Size: 682/4096 entries
    8206 total entries added
    95545 aging polls, last aging poll occurred 3 seconds ago
```

The following is sample output from an AOS product with an Ethernet interface and a point-to-point interface configured for ITM:

```
#show ip flow interface
eth 0/1
    ip flow ingress
ppp 1
    ip flow ingress
    ip flow egress
```


show ip flow top-talkers

Use the **show ip flow top-talkers** command to view information pertinent to integrated traffic monitoring (ITM) Top Talker configuration and to reveal possible configuration problems. Variations of this command include:

show ip flow top-talkers
show ip flow top-talkers day
show ip flow top-talkers day detail
show ip flow top-talkers hour
show ip flow top-talkers hour detail
show ip flow top-talkers port
show ip flow top-talkers port detail

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines after.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

day	Optional. Specifies the display of Top Talker data for the current 24-hour period.
hour	Optional. Specifies the display of Top Talker data for the current hour.
port	Optional. Specifies the display of Top Talker monitored port traffic for the current interval.
detail	Optional. Specifies the display of information for previous and current intervals.

Default Values

No default values are necessary for this command.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following is sample output from the **show ip flow top-talkers** command:

#show ip flow top-talkers

Current Interval Top Talkers:
1:00 PM to 1:15 PM

Top Traffic Sources:		Top Traffic Destinations:	
IP Address	Packets	IP Address	Packets
10.100.43.254	1451	10.22.162.3	735
10.100.43.161	860	10.22.166.222	707
10.22.160.253	384	10.22.160.7	407
10.100.43.200	292	224.0.0.6	393
10.22.165.17	222	10.22.130.6	391

Top 5 talkers shown. 742 flows processed.

show ip igmp groups

Use the **show ip igmp groups** command to display the multicast groups that have been registered by directly connected receivers using Internet Group Management Protocol (IGMP). If no multicast group IP address is specified, all groups are shown with this command. Variations of this command include:

show ip igmp groups
show ip igmp groups *<multicast address>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<multicast address>	Optional. Displays the IP address of a multicast group. The multicast group IP address range is **244.0.0.0** to **239.255.255.255** or **224.0.0.0 /4**.

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from this command:

```
>enable
#show ip igmp groups
IGMP Connected Group Membership
Group Address   Interface       Uptime    Expires   Last Reported
172.0.1.50      Loopback100     00:42:57  00:02:50  172.23.23.1
172.1.1.1       Ethernet0/1     00:05:26  00:02:51  1.1.1.2
172.1.1.1       Loopback100     00:42:57  00:02:51  172.23.23.1
```

show ip igmp interface

Use the **show ip igmp interface** command to display multicast-related information per-interface. If no interface is specified, this command shows information for all interfaces. Variations of this command include:

show ip igmp interface
show ip igmp interface <*interface*>

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*interface*>	Optional. Displays information for a specific interface type. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Enter the **show ip igmp interface ?** command for a complete list of interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Usage Examples

The following example is sample output from the **show ip igmp interface** command:

```
>enable
#show ip igmp interface
eth 0/1 is UP
 Ip Address is 10.22.120.47, netmask is 255.255.255.0
 IGMP is enabled on interface
 Current IGMP version is 2
 IGMP query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Last member query count is 2
 Last member query response interval is 1000 ms
 IGMP activity: 548 joins, 0 leaves
 IGMP querying router is 0.0.0.0
 IGMP helper address is disabled
```

show ip igmp snooping

Use the **show ip igmp snooping** command to display Internet Group Management Protocol (IGMP) snooping information. Variations of this command include:

show ip igmp snooping
show ip igmp snooping mrouter
show ip igmp snooping mrouter vlan <*vlan id*>
show ip igmp snooping vlan
show ip igmp snooping vlan <*vlan id*>

Global IGMP snooping overrides the virtual local area network (VLAN) IGMP snooping. If global snooping is disabled, you cannot enable VLAN IGMP snooping. If global snooping is enabled, you can enable or disable VLAN IGMP snooping. Refer to *ip igmp snooping on page 1407* *for more information.*

The output of all ***show*** *commands can be limited by appending the following modifiers to the end of the command:* **|** ***begin*** <*text*>, **|** ***exclude*** <*text*>, *and* **|** ***include*** <*text*>. *The* ***include*** *modifier limits output to lines that contain the specified text, the* ***exclude*** *modifier excludes any lines with the specified text, and the* ***begin*** *modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the *Enable Mode Command Set on page 94*.

Syntax Description

mrouter	Optional. Displays the ports associated with multicast routers.
vlan	Optional. Displays whether IGMP snooping is enabled or disabled for all VLANs.
vlan <*vlan id*>	Optional. Displays whether IGMP snooping is enabled or disabled for a particular VLAN.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip igmp snooping vlan** command:

```
>enable
#show ip igmp snooping vlan 1
Vlan 1: IGMP snooping is enabled on this VLAN
```

The following is sample output from the **show ip igmp snooping mrouter vlan** command:

```
>enable
#show ip igmp snooping mrouter vlan 200
VLAN            Ports
----------------+ ---------------------------------
 200            Gi0/2(static)
```

show ip interfaces

Use the **show ip interfaces** command to display the status information for all Internet Protocol version 4 (IPv4) interfaces (or a specific IPv4 interface). Variations of this command include:

show ip interfaces
show ip interfaces *<ipv4 interface>*
show ip interfaces *<ipv4 interface>* **brief**
show ip interfaces efm-group *<group id>*
show ip interfaces mef-ethernet *<slot/port>*
show ip interfaces system-control-evc
show ip interfaces system-management-evc

*To view secondary IP addresses, use the **show running-config** command.*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv4 interface>	Optional. Displays status information for a specific IPv4 interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show ip interfaces ?** for a complete list of applicable interfaces. If no interface is specified, status information for all interfaces is displayed.
efm-group *<group id>*	Specifies an Ethernet in the first mile (EFM) group ID. Range is **1** to **1024**.
mef-ethernet *<slot/port>*	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Displays status information for the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Displays status information for the system management EVC.
brief	Optional. Displays an abbreviated version of interface statistics for all IPv4 interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 11.1	Demand interface was added.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.4.0	Command was expanded to include the virtual local area network (VLAN) interface.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R11.3.0	Command was expanded to include the Ethernet in the first mile (EFM) group and Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following is sample output of the **show ip interfaces** command, and displays information for IPv4 interfaces:

```
>enable
#show ip interfaces
eth 0/1 is UP, line protocol is UP
 Ip address is 10.10.10.1
 Netmask is 255.255.255.0
 MTU is 1500
 Fastcaching is Enabled
 RIP Authentication is Disabled
 RIP Tx uses global version value
```

show ip local policy

Use the **show ip local policy** command to display information about the route-map used for local policy-based routing. Variations of this command include the following:

show ip local policy
show ip local policy vrf <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

vrf <*name*>	Optional. Displays information for only the specified virtual routing and forwarding (VRF).

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output (just for the default VRF) from this command:

```
>enable
#show ip local policy
Local policy routing is enabled, using route-map SAMPLE_RTEMAP
route-map SAMPLE_RTEMAP, permit, sequence 1
 Match clauses:
   ip address (access-lists): SAMPLE_ACL
 Set clauses:
 BGP Filtering matches: 0 routes
 Policy routing matches: 0 packets 0 bytes
 Redistribution Filtering matches: 0 routes
```

show ip nhrp

Use the **show ip nhrp** command to display Next Hop Resolution Protocol (NHRP) cache entries. Variations of this command include:

show ip nhrp
show ip nhrp brief
show ip nhrp interface tunnel <*number*>
show ip nhrp interface tunnel <*number*> **brief**
show ip nhrp <*ip address*>
show ip nhrp <*ip address*> **brief**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

brief	Optional. Shortens the output for each entry to fit on a single line.
interface tunnel <*number*>	Optional. Limits entries to only those that correspond to the specified interface.
<*ip address*>	Optional. Limits entries to those with the specified private tunnel IP address. Express IP addresses in dotted decimal notation; for example, **10.10.10.1**.

Command History

Release R11.9.0	Command was introduced.

Usage Examples

The following example displays all NHRP cache entries:

```
>enable
#show ip nhrp
Interface tunnel 1:
    Protocol address: 10.10.10.1/32,
    Type: static, Flags: unique,
    NMBA Address: 1.1.1.1
    Created: 33:44:55, Expires: Never
```


show ip mroute

Use the **show ip mroute** command to display IP multicasting routing table information. Variations of this command include:

show ip mroute
show ip mroute all
show ip mroute *<ip address>*
show ip mroute *<interface>*
show ip mroute summary

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

all	Optional. Displays all multicast routes, including those not used to forward multicast traffic.
<ip address>	Optional. Displays IP address of a multicast group. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<interface>	Optional. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show ip mroute ?** for a complete list of interfaces.
summary	Optional. Displays a single-line summary for each entry in the IP multicast routing table.

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 11.1	The **all** parameter was added.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Usage Examples

The following is sample output from the **show ip mroute all** command:

```
>enable
#show ip mroute all
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned, J - Join SPT, T - SPT-bit Set,
F - Register, R - RP-bit Set
Timers: Uptime/Expires
(*, 225.1.0.1), 01:17:34/00:03:25, RP 192.168.0.254, Flags: SC
 Forwarding Entry: Yes
 Incoming interface: tunnel 2, RPF nbr 172.16.2.10
 Outgoing interface list:
   eth 0/1, Forward, 01:17:34/00:03:25
```


show ip nhrp nhs

Use the **show ip nhrp nhs** command to display a list of configured next-hop server (NHS) servers and their statuses for each Next Hop Resolution Protocol (NHRP) interface. Variations of this command include:

show ip nhrp nhs
show ip nhrp interface tunnel <*number*> **nhs**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interface tunnel <*number*>	Optional. Specifies that output is limited to a single tunnel interface.

Default Values

No default values are necessary for this command.

Command History

Release R11.7.0	Command was introduced.

Usage Examples

The following example displays the NHS servers and their statuses for all configured NHRP interfaces:

```
>enable
#show ip nhrp nhs
INTERFACE          NHS          STATUS
tunnel 4           1.1.1.2      UP
tunnel 5           5.5.5.5      DOWN
```


show ip nhrp traffic

Use the **show ip nhrp traffic** command to display the Next Hop Resolution Protocol (NHRP) traffic for all tunnel interfaces. Variations of this command include:

show ip nhrp traffic
show ip nhrp interface tunnel <*number*> **traffic**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

interface tunnel <*number*>	Optional. Specifies that output is limited to a single tunnel interface.

Default Values

No default values are necessary for this command.

Command History

Release R11.7.0	Command was introduced.

Usage Examples

The following example displays NHRP traffic statistics for the tunnel interface **1**:

```
>enable
#show ip nhrp interface tunnel 1 traffic
Interface tunnel 1:
    Sent: 1234567890 Total
          1234567890 Resolution Requests Resolution Replies:
          1234567890 Total, 1234567890 Acknowledged,
          1234567890 Prohibited, 1234567890 Insufficient Resources,
          1234567890 No Binding, 1234567890 Not Unique
          1234567890 Registration Requests Registration Replies:
          1234567890 Total, 1234567890 Acknowledged,
          1234567890 Prohibited, 1234567890 Insufficient Resources,
          1234567890 Already Registered
          1234567890 Purge Requests
          1234567890 Purge Replies Error Indications:
          1234567890 Total, 1234567890 Unrecognized Extension,
          1234567890 Loop Detected, 1234567890 Protocol Address Unreachable,
```


1234567890 Protocol Error, 1234567890 SDU Size Exceeded,
1234567890 Invalid Extension, 1234567890 Authentication Failure,
1234567890 Hop Count Exceeded

Received: 1234567890 Total
1234567890 Resolution Requests Resolution Replies:
1234567890 Total, 1234567890 Acknowledged,
1234567890 Prohibited, 1234567890 Insufficient Resources,
1234567890 No Binding, 1234567890 Not Unique
1234567890 Registration Requests
Registration Replies:
1234567890 Total, 1234567890 Acknowledged,
1234567890 Prohibited, 1234567890 Insufficient Resources,
1234567890 Already Registered
1234567890 Purge Requests
1234567890 Purge Replies
Error Indications:
1234567890 Total, 1234567890 Unrecognized Extension,
1234567890 Loop Detected, 1234567890 Protocol Address Unreachable,
1234567890 Protocol Error, 1234567890 SDU Size Exceeded,
1234567890 Invalid Extension, 1234567890 Authentication Failure,
1234567890 Hop Count Exceeded

show ip ospf

Use the **show ip ospf** command to display general information regarding Open Shortest Path First version 2 (OSPFv2) processes. Variations of this command include:

show ip ospf
show ip ospf *<process id>*

> NOTE *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv2 process. Valid range is **1** to **65535**.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.3.0	Command was expanded to include the *<process id>* parameter.

Usage Examples

The following is sample output from the **show ip ospf** command:

```
>enable
#show ip ospf
Summary of OSPF Process with ID: 192.2.72.101
 Supports only single Type Of Service routes (TOS 0)
 SPF delay timer: 5 seconds, Hold time between SPFs: 10 seconds
 LSA interval: 240 seconds
 Number of external LSAs: 0, Checksum Sum: 0x0
 Number of areas: 0, normal: 0, stub: 0, NSSA: 0
```


show ip ospf database

Use the **show ip ospf database** command to display information from the Open Shortest Path First version 2 (OSPFv2) database regarding a specific router. There are several variations of this command that can be used to obtain information about different OSPF link state advertisements. The variations are shown below:

show ip ospf database
show ip ospf database adv-router *<router id>*
show ip ospf database database-summary
show ip ospf database self-originate
show ip ospf *<process id>* **database**
show ip ospf *<process id>* **database adv-router** *<router id>*
show ip ospf *<process id>* **database database-summary**
show ip ospf *<process id>* **database self-originate**
show ip ospf *<process id>* *<area id>* **database**
show ip ospf *<process id>* *<area id>* **database adv-router** *<router id>*
show ip ospf *<process id>* *<area id>* **database database-summary**
show ip ospf *<process id>* *<area id>* **database self-originate**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<area id>	Optional. Specifies an OSPF area ID. Refer to *network <ipv4 address> <wildcard mask> area <area id> on page 4133* for more information.
<process id>	Optional. Limits the output of this command to a single OSPFv2 process. Valid range is **1** to **65535**.
adv-router *<router id>*	Optional. Optional. Limits the output of this command to a single specified advertising router.
database-summary	Optional. Displays a simplified list of LSAs for the specified area.
self-originate	Optional. Displays information about LSAs originated from this router.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Release R11.3.0	Command was expanded to include the <*process id*> and **self-originate** parameters.

Usage Examples

The following example shows the database link state summary for all areas:

>**enable**
#show ip ospf 61 database
OSPF router with ID: 9.8.8.1 (Process ID 61, VRF RED)

Router Link States, Area 0

Adv Router	Age	Seq #	Checksum	Link count	Bits
9.8.8.1	1705	0x80000093	0x065E	1	None
192.168.120.200	895	0x80000087	0x6271	1	B

Net Link States, Area 0

Adv Router	Age	Seq #	Checksum	Rtr Count
192.168.120.2	895	0x80000081	0x0643	2

Summary Net Link States, Area 0

Adv Router	Age	Seq #	Checksum	Prefix/Link ID
9.8.8.1	31	0x80000091	0x0F99	9.8.8.1
192.168.120.200	895	0x80000081	0xDE9C	192.168.120.0

Router Link States, Area 1

Adv Router	Age	Seq #	Checksum	Link count	Bits
9.8.8.1	1769	0x80000095	0xE95A	2	None

Summary Net Link States, Area 1

Adv Router	Age	Seq #	Checksum	Prefix/Link ID
9.8.8.1	31	0x80000091	0x4ED6	10.24.106.0
9.8.8.1	600	0x80000090	0xB11E	192.168.120.0
9.8.8.1	600	0x80000090	0x4015	200.200.200.2

Type 5 AS External Net Link States

Adv Router	Age	Seq #	Checksum	Prefix/Link ID
9.8.8.1	670	0x80000091	0x69CA	0.0.0.0
9.8.8.1	30	0x80000091	0xBBDA	10.24.204.128

show ip ospf database asbr-summary

Use the **show ip ospf database asbr-summary** command to display information from the Open Shortest Path First version 2 (OSPFv2) database regarding a specific router. There are several variations of this command that can be used to obtain information about different OSPF link state advertisements. The variations are shown below:

show ip ospf database asbr-summary
show ip ospf database asbr-summary <*link-state id*>
show ip ospf database asbr-summary <*link-state id*> **adv-router** <*router id*>
show ip ospf database asbr-summary <*link-state id*> **adv-router** <*router id*> **internal**
show ip ospf database asbr-summary <*link-state id*> **internal**
show ip ospf database asbr-summary <*link-state id*> **self-originate**
show ip ospf database asbr-summary <*link-state id*> **self-originate internal**
show ip ospf database asbr-summary adv-router <*router id*>
show ip ospf database asbr-summary adv-router <*router id*> **internal**
show ip ospf database asbr-summary internal
show ip ospf database asbr-summary self-originate
show ip ospf database asbr-summary self-originate internal
show ip ospf <*process id*> **database asbr-summary**
show ip ospf <*process id*> **database asbr-summary** <*link-state id*>
show ip ospf <*process id*> **database asbr-summary** <*link-state id*> **adv-router** <*router id*>
show ip ospf <*process id*> **database asbr-summary** <*link-state id*> **adv-router** <*router id*> **internal**
show ip ospf <*process id*> **database asbr-summary** <*link-state id*> **internal**
show ip ospf <*process id*> **database asbr-summary** <*link-state id*> **self-originate**
show ip ospf <*process id*> **database asbr-summary** <*link-state id*> **self-originate internal**
show ip ospf <*process id*> **database asbr-summary adv-router** <*router id*>
show ip ospf <*process id*> **database asbr-summary adv-router** <*router id*> **internal**
show ip ospf <*process id*> **database asbr-summary internal**
show ip ospf <*process id*> **database asbr-summary self-originate**
show ip ospf <*process id*> **database asbr-summary self-originate internal**
show ip ospf <*process id*> <*area id*> **database asbr-summary**
show ip ospf <*process id*> <*area id*> **database asbr-summary** <*link-state id*>
show ip ospf <*process id*> <*area id*> **database asbr-summary** <*link-state id*> **adv-router** <*router id*>
show ip ospf <*process id*> <*area id*> **database asbr-summary** <*link-state id*> **adv-router** <*router id*> **internal**
show ip ospf <*process id*> <*area id*> **database asbr-summary** <*link-state id*> **internal**
show ip ospf <*process id*> <*area id*> **database asbr-summary** <*link-state id*> **self-originate**
show ip ospf <*process id*> <*area id*> **database asbr-summary** <*link-state id*> **self-originate internal**
show ip ospf <*process id*> <*area id*> **database asbr-summary adv-router** <*router id*>
show ip ospf <*process id*> <*area id*> **database asbr-summary adv-router** <*router id*> **internal**
show ip ospf <*process id*> <*area id*> **database asbr-summary internal**
show ip ospf <*process id*> <*area id*> **database asbr-summary self-originate**
show ip ospf <*process id*> <*area id*> **database asbr-summary self-originate internal**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<area id>	Optional. Specifies an OSPF area ID. Refer to *network <ipv4 address> <wildcard mask> area <area id> on page 4133* for more information.
<link-state id>	Optional. Displays information from a specific link state ID. The value defined in this field is tied to the advertisement's loop start (LS) type.
<process id>	Optional. Limits the output of this command to a single OSPFv2 process. Valid range is **1** to **65535**.
adv-router *<router id>*	Optional. Optional. Limits the output of this command to a single specified advertising router.
internal	Optional. Displays the shortest path first (SPF) calculation results for the LSAs and whether the LAS was used in route calculation.
self-originate	Optional. Displays information about LSAs originated from this router.

Default Values

No default values are necessary for this command.

Command History

Release R11.3.0	Command was introduced.

Functional Notes

The link state ID differs depending on whether the LSA in question describes a network or a router.

If describing a network, the link state ID is one of the following:

- The network's IP address. This is true for type 3 summary link advertisements and in autonomous system external link advertisements.
- An address obtained from the link state ID. If the network link advertisement's link state ID is masked with the network's subnet mask, this will yield the network's IP address.

If describing a router, the link state ID is always the router's OSPF router ID.

Usage Examples

The following is sample output from the **show ip ospf database asbr-summary** command:

```
>enable
#show ip ospf 1 0 database asbr-summary
```


OSPF router with ID: 35.35.35.35 (Process ID 1)

Summary ASB Link States, Area 0

Link State age: 153
Link State type: Summary-ASB-LSA (0x0004)
Link State ID: 2.2.2.2
Advertising Router: 92.92.92.92
Sequence Number: 0x800003CC
Checksum: 0xA170
Options:
Length: 28
Metric: 2

show ip ospf database external

Use the **show ip ospf external** command to display Open Shortest Path First version 2 (OSPFv2) information for external link state advertisements (LSAs). Variations of this command include:

show ip ospf database external
show ip ospf database external *<link-state id>*
show ip ospf database external *<link-state id>* **adv-router** *<router id>*
show ip ospf database external *<link-state id>* **self-originate**
show ip ospf database external adv-router *<router id>*
show ip ospf database external self-originate
show ip ospf *<process id>* **database external**
show ip ospf *<process id>* **database external** *<link-state id>*
show ip ospf *<process id>* **database external** *<link-state id>* **adv-router** *<router id>*
show ip ospf *<process id>* **database external** *<link-state id>* **self-originate**
show ip ospf *<process id>* **database external adv-router** *<router id>*
show ip ospf *<process id>* **database external self-originate**
show ip ospf *<process id>* *<area id>* **database external**
show ip ospf *<process id>* *<area id>* **database external** *<link-state id>*
show ip ospf *<process id>* *<area id>* **database external** *<link-state id>* **adv-router** *<router id>*
show ip ospf *<process id>* *<area id>* **database external** *<link-state id>* **self-originate**
show ip ospf *<process id>* *<area id>* **database external adv-router** *<router id>*
show ip ospf *<process id>* *<area id>* **database external self-originate**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<area id>	Optional. Specifies an OSPF area ID. Refer to *network <ipv4 address> <wildcard mask> area <area id> on page 4133* for more information.
<link-state id>	Optional. Displays information from a specific link state ID. The value defined in this field is tied to the advertisement's loop start (LS) type.
<process id>	Optional. Limits the output of this command to a single OSPFv2 process. Valid range is **1** to **65535**.
adv-router *<router id>*	Optional. Optional. Limits the output of this command to a single specified advertising router.
self-originate	Optional. Displays information about LSAs originated from this router.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.3.0	Command was expanded to include the <*process id*>, and **self-originate** parameters.

Functional Notes

The link state ID differs depending on whether the LSA in question describes a network or a router.

If describing a network, the link state ID is one of the following:

- The network's IP address. This is true for type 3 summary link advertisements and in autonomous system external link advertisements.
- An address obtained from the link state ID. If the network link advertisement's link state ID is masked with the network's subnet mask, this will yield the network's IP address.

If describing a router, the link state ID is always the router's OSPF router ID.

Usage Examples

The following is sample output from the **show ip ospf database external** command:

```
>enable
#show ip ospf 61 database external

    OSPF router with ID: 9.8.8.1 (Process ID 61, VRF RED)
            Type 5 AS External Net Link States
                Link State age: 1626
                Link State type: AS External (0x0005)
                Link State ID: 0.0.0.0
                Advertising Router: 9.8.8.1
                Sequence Number: 0x80000093
                Checksum: 0x65CC
                Options: E
                Length: 36
    Network Mask: 255.255.255.255
                Metric Type: 1 (Comparable directly to link state metric)
                Metric: 22222
                Forward Address: 10.24.106.2
                External Route Tag: 0x00000000
```

show ip ospf database network

Use the **show ip ospf database network** command to display Open Shortest Path First version 2 (OSPFv2) information for network links state advertisements (LSAs). Variations of this command include:

show ip ospf database network
show ip ospf database network *<link-state id>*
show ip ospf database network *<link-state id>* **adv-router** *<router id>*
show ip ospf database network *<link-state id>* **self-originate**
show ip ospf database network adv-router *<router id>*
show ip ospf database network self-originate
show ip ospf *<process id>* **database network**
show ip ospf *<process id>* **database network** *<link-state id>*
show ip ospf *<process id>* **database network** *<link-state id>* **adv-router** *<router id>*
show ip ospf *<process id>* **database network** *<link-state id>* **self-originate**
show ip ospf *<process id>* **database network adv-router** *<router id>*
show ip ospf *<process id>* **database network self-originate**
show ip ospf *<process id>* *<area id>* **database network**
show ip ospf *<process id>* *<area id>* **database network** *<link-state id>*
show ip ospf *<process id>* *<area id>* **database network** *<link-state id>* **adv-router** *<router id>*
show ip ospf *<process id>* *<area id>* **database network** *<link-state id>* **self-originate**
show ip ospf *<process id>* *<area id>* **database network adv-router** *<router id>*
show ip ospf *<process id>* *<area id>* **database network self-originate**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<area id>	Optional. Specifies an OSPF area ID. Refer to *network <ipv4 address> <wildcard mask> area <area id> on page 4133* for more information.
<link-state id>	Optional. Displays information from a specific link state ID. The value defined in this field is tied to the advertisement's loop start (LS) type.
<process id>	Optional. Limits the output of this command to a single OSPFv2 process. Valid range is **1** to **65535**.
adv-router *<router id>*	Optional. Optional. Limits the output of this command to a single specified advertising router.
self-originate	Optional. Displays information about LSAs originated from this router.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.3.0	Command was expanded to include the <*process id*>, and **self-originate** parameters.

Functional Notes

The link state ID differs depending on whether the LSA in question describes a network or a router.

If describing a network, the link state ID is one of the following:

- The network's IP address. This is true for type 3 summary link advertisements and in autonomous system external link advertisements.
- An address obtained from the link state ID. If the network link advertisement's link state ID is masked with the network's subnet mask, this will yield the network's IP address.

If describing a router, the link state ID is always the router's OSPF router ID.

Usage Examples

The following is sample output from the **show ip ospf database network** command:

```
>enable
#show ip ospf 61 database network
  OSPF router with ID: 9.8.8.1 (Process ID 61, VRF RED)

    Network Link States, Area 0

      Link State age: 60
      Link State type: Network-LSA (0x0002)
      Link State ID: 10.24.106.10
      Advertising Router: 9.8.8.1
      Sequence Number: 0x80000002
      Checksum: 0x3282
      Options: E
      Length: 32
        Network Mask: 255.255.255.0
        Number of Attached Routers: 2
          Attached Router: 9.8.8.1
          Attached Router: 4.4.4.4
```

show ip ospf database router

Use the **show ip ospf database router** command to display Open Shortest Path First version 2 (OSPFv2) information for router link state advertisements (LSAs). Variations of this command include:

show ip ospf database router
show ip ospf database router <*link-state id*>
show ip ospf database router <*link-state id*> **adv-router** <*router id*>
show ip ospf database router <*link-state id*> **adv-router** <*router id*> **internal**
show ip ospf database router <*link-state id*> **internal**
show ip ospf database router <*link-state id*> **self-originate**
show ip ospf database router <*link-state id*> **self-originate internal**
show ip ospf database router adv-router <*router id*>
show ip ospf database router adv-router <*router id*> **internal**
show ip ospf database router internal
show ip ospf database router self-originate
show ip ospf database router self-originate internal
show ip ospf <*process id*> **database router**
show ip ospf <*process id*> **database router** <*link-state id*>
show ip ospf <*process id*> **database router** <*link-state id*> **adv-router** <*router id*>
show ip ospf <*process id*> **database router** <*link-state id*> **adv-router** <*router id*> **internal**
show ip ospf <*process id*> **database router** <*link-state id*> **internal**
show ip ospf <*process id*> **database router** <*link-state id*> **self-originate**
show ip ospf <*process id*> **database router** <*link-state id*> **self-originate internal**
show ip ospf <*process id*> **database router adv-router** <*router id*>
show ip ospf <*process id*> **database router adv-router** <*router id*> **internal**
show ip ospf <*process id*> **database router internal**
show ip ospf <*process id*> **database router self-originate**
show ip ospf <*process id*> **database router self-originate internal**
show ip ospf <*process id*> <*area id*> **database router**
show ip ospf <*process id*> <*area id*> **database router** <*link-state id*>
show ip ospf <*process id*> <*area id*> **database router** <*link-state id*> **adv-router** <*router id*>
show ip ospf <*process id*> <*area id*> **database router** <*link-state id*> **adv-router** <*router id*> **internal**
show ip ospf <*process id*> <*area id*> **database router** <*link-state id*> **internal**
show ip ospf <*process id*> <*area id*> **database router** <*link-state id*> **self-originate**
show ip ospf <*process id*> <*area id*> **database router** <*link-state id*> **self-originate internal**
show ip ospf <*process id*> <*area id*> **database router adv-router** <*router id*>
show ip ospf <*process id*> <*area id*> **database router adv-router** <*router id*> **internal**
show ip ospf <*process id*> <*area id*> **database router internal**
show ip ospf <*process id*> <*area id*> **database router self-originate**
show ip ospf <*process id*> <*area id*> **database router self-originate internal**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<area id>	Optional. Specifies an OSPF area ID. Refer to *network <ipv4 address> <wildcard mask> area <area id> on page 4133* for more information.
<link-state id>	Optional. Displays information from a specific link state ID. The value defined in this field is tied to the advertisement's loop start (LS) type.
<process id>	Optional. Limits the output of this command to a single OSPFv2 process. Valid range is **1** to **65535**.
adv-router *<router id>*	Optional. Optional. Limits the output of this command to a single specified advertising router.
internal	Optional. Displays the shortest path first (SPF) calculation results for the LSAs and whether the LAS was used in route calculation.
self-originate	Optional. Displays information about LSAs originated from this router.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.3.0	Command was expanded to include the *<process id>*, **internal**, and **self-originate** parameters.

Functional Notes

The link state ID differs depending on whether the LSA in question describes a network or a router.

If describing a network, the link state ID is one of the following:

- The network's IP address. This is true for type 3 summary link advertisements and in autonomous system external link advertisements.
- An address obtained from the link state ID. If the network link advertisement's link state ID is masked with the network's subnet mask, this will yield the network's IP address.

If describing a router, the link state ID is always the router's OSPF router ID.

Usage Examples

The following is sample output from the **show ip ospf database router** command:

```
>enable
#show ip ospf 61 database router
OSPF router with ID: 9.8.8.1 (Process ID 61, VRF RED)

  Router Link States, Area 0

    Link State age: 350
    Link State type: Router-LSA (0x0001)
    Link State ID: 9.8.8.1
    Advertising Router: 9.8.8.1
    Sequence Number: 0x8000009D
    Checksum: 0x4210
    Options: E
    Length: 40
      Flags: Area Border Router, AS Boundary Router
      Number of Links: 1
        Link connected to: Transit network Link
          (Link ID} Designated Router address: 5.5.5.5
          (Link Data) Router Interface address: 9.8.8.1
          TOS 0 Metric: 1
```


show ip ospf database summary

Use the **show ip ospf database summary** command to display Open Shortest Path First version 2 (OSPFv2) information for summary link state advertisements (LSAs). Variations of this command include:

show ip ospf database summary
show ip ospf database summary *<link-state id>*
show ip ospf database summary *<link-state id>* **adv-router** *<router id>*
show ip ospf database summary *<link-state id>* **self-originate**
show ip ospf database summary adv-router *<router id>*
show ip ospf database summary self-originate
show ip ospf *<process id>* **database summary**
show ip ospf *<process id>* **database summary** *<link-state id>*
show ip ospf *<process id>* **database summary** *<link-state id>* **adv-router** *<router id>*
show ip ospf *<process id>* **database summary** *<link-state id>* **self-originate**
show ip ospf *<process id>* **database summary adv-router** *<router id>*
show ip ospf *<process id>* **database summary self-originate**
show ip ospf *<process id>* *<area id>* **database summary**
show ip ospf *<process id>* *<area id>* **database summary** *<link-state id>*
show ip ospf *<process id>* *<area id>* **database summary** *<link-state id>* **adv-router** *<router id>*
show ip ospf *<process id>* *<area id>* **database summary** *<link-state id>* **self-originate**
show ip ospf *<process id>* *<area id>* **database summary adv-router** *<router id>*
show ip ospf *<process id>* *<area id>* **database summary self-originate**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<area id>	Optional. Specifies an OSPF area ID. Refer to *network <ipv4 address> <wildcard mask> area <area id> on page 4133* for more information.
<link-state id>	Optional. Displays information from a specific link state ID. The value defined in this field is tied to the advertisement's loop start (LS) type.
<process id>	Optional. Limits the output of this command to a single OSPFv2 process. Valid range is **1** to **65535**.
adv-router *<router id>*	Optional. Optional. Limits the output of this command to a single specified advertising router.
self-originate	Optional. Displays information about LSAs originated from this router.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.3.0	Command was expanded to include the <*process id*>, and **self-originate** parameters.

Functional Notes

The link state ID differs depending on whether the LSA in question describes a network or a router.

If describing a network, the link state ID is one of the following:

- The network's IP address. This is true for type 3 summary link advertisements and in autonomous system external link advertisements.
- An address obtained from the link state ID. If the network link advertisement's link state ID is masked with the network's subnet mask, this will yield the network's IP address.

If describing a router, the link state ID is always the router's OSPF router ID.

Usage Examples

The following is sample output from the **show ip ospf database summary** command:

```
>enable
#show ip ospf 61 database summary
  OSPF router with ID: 9.8.8.1 (Process ID 61, VRF RED)

    Summary Net Link States, Area 1

      Link State age: 689
      Link State type: Summary Network (0x0003)
      Link State ID: 10.24.106.0
      Advertising Router: 9.8.8.1
      Sequence Number: 0x80000009
      Checksum: 0x5F4E
      Options: E
      Length: 28
        Network Mask: /24
        Metric: 1
```


show ip ospf interface

Use the **show ip ospf interface** command to display Open Shortest Path First version 2 (OSPFv2) information for a specific interface. Variations of this command include:

show ip ospf interface
show ip ospf interface *<interface>*
show ip ospf interface system-control-evc
show ip ospf interface system-management-evc

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Optional. Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show ip ospf interface ?** for a complete list of applicable interfaces.
system-control-evc	Optional. Displays OSPF information for the system control Ethernet virtual connection (EVC)
system-management-evc	Optional. Displays OSPF information for the system management EVC.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.3.0	Command was expanded to include the demand and Ethernet in the first mile (EFM) group interfaces and the **system-control-evc** and **system-management-evc** parameters.

Usage Examples

The following example shows OSPF information for the PPP 1 interface.

```
>enable
#show ip ospf 61 interface
eth 0/1.106 is UP, line protocol is UP
  IP address: 10.24.106.10 255.255.255.0, Area: 0
  Process ID 61, Router ID: 9.8.8.1, Network type: Broadcast, Cost: 1
  Transmit delay: 1, State: DR, Priority: 1
  Designated Router (ID): 9.8.8.1, Interface Address: 10.24.106.10
  Backup Designated Router (ID): 200.200.200.2, Interface Address: 10.24.106.2
  Timer intervals: Hello: 10, Dead: 40, Retransmit: 5
    Hello due in: 00:00:08
  Number of neighbors: 1, Adjacent neighbors: 1
    Adjacent with neighbor: 200.200.200.2 (Backup Designated Router)
loop 97 is UP, line protocol is UP
  IP address: 9.8.7.1 255.255.255.0, Area: 1
  Process ID 61, Router ID: 9.8.8.1, Network type: Point-to-point, Cost: 1
  Transmit delay: 1, State: PTPT, Priority: 1
  Timer intervals: Hello: 10, Dead: 40, Retransmit: 5
    Hello due in: 00:00:10
  Number of neighbors: 0, Adjacent neighbors: 0
loop 98 is UP, line protocol is UP
  IP address: 9.8.8.1 255.255.255.0, Area: 1
  Process ID 61, Router ID: 9.8.8.1, Network type: Point-to-point, Cost: 1
  Transmit delay: 1, State: PTPT, Priority: 1
  Timer intervals: Hello: 10, Dead: 40, Retransmit: 5
    Hello due in: 00:00:10
  Number of neighbors: 0, Adjacent neighbors: 0
```


show ip ospf neighbor

Use the **show ip ospf neighbor** command to display Open Shortest Path First version 2 (OSPFv2) neighbor information for a specific interface. Variations of this command include:

show ip ospf neighbor
show ip ospf neighbor detail
show ip ospf neighbor *<interface>*
show ip ospf neighbor *<interface>* **detail**
show ip ospf neighbor *<interface>* *<neighbor id>*
show ip ospf neighbor *<interface>* *<neighbor id>* **detail**
show ip ospf neighbor *<neighbor id>*
show ip ospf neighbor *<neighbor id>* **detail**
show ip ospf neighbor system-control-evc
show ip ospf neighbor system-control-evc detail
show ip ospf neighbor system-control-evc *<neighbor id>*
show ip ospf neighbor system-control-evc *<neighbor id>* **detail**
show ip ospf neighbor system-management-evc
show ip ospf neighbor system-management-evc detail
show ip ospf neighbor system-management-evc *<neighbor id>*
show ip ospf neighbor system-management-evc *<neighbor id>* **detail**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Optional. Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show ip ospf neighbor ?** for a complete list of applicable interfaces.
<neighbor id>	Optional. Specifies a specific neighbor's router ID.
detail	Optional. Displays detailed information on neighbors.
system-control-evc	Optional. Displays OSPF neighbor information for the system control Ethernet virtual connection (EVC)
system-management-evc	Optional. Displays OSPF neighbor information for the system management EVC.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.3.0	Command expanded to include the asynchronous transfer mode (ATM), bridged virtual interface (BVI), demand, Ethernet in the first mile (EFM) group, Gigabit Ethernet, and loopback interfaces. The command was also expanded to include the **system-control-evc** and **system-management-evc** parameters.

Usage Examples

The following example shows detailed information on the OSPF neighbors:

>**enable**
#show ip ospf neighbor
OSPF router with ID: 9.8.8.1, **Process ID 61, VRF RED**

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
204.204.204.61	1	FULL/BDR	00:00:38	20	eth 0/1.106

show ip ospf summary-address

Use the **show ip ospf summary-address** command to display a list of all summary address redistribution information for the system.Variations of this command include:

show ip ospf summary-address

show ip ospf *<process id>* **summary-address**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.3.0	Command was expanded to include the *<process id>* parameter.

Usage Examples

The following example displays the summary address redistribution information for process **61**:

```
>enable
#show ip ospf 61 summary-address
OSPF Summary Addresses, Process ID 61, VRF RED:
  8.7.0.0/255.255.0.0 Metric 11111, Type 1, advertise
```


show ip pim-sparse

Use the **show ip pim-sparse** command to display protocol-independent multicast (PIM) configuration information. Sparse mode or PIM-SM is a routing protocol used to establish and maintain the multicast distribution tree. Routers can participate in the shared tree (RPT) rooted at the rendezvous point (RP) router or the shortest path tree (SPT) rooted at a multicast source. PIM-SM also establishes both shared trees and SPTs. Variations of this command include:

show ip pim-sparse
show ip pim-sparse interfaces *<interface>*
show ip pim-sparse neighbor
show ip pim-sparse rp-map
show ip pim-sparse rp-set
show ip pim-sparse state
show ip pim-sparse traffic

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

interfaces *<interface>*	Optional. Displays PIM-SM configuration and status information for a specific interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show ip pim-sparse interface ?** to display a list of applicable interfaces.
neighbor	Optional. Displays neighbor adjacency information.
rp-map	Optional. Displays active group-to-RP mappings.
rp-set	Optional. Displays a list of statically configured RP candidates. The multicast group IP address is **224.0.0.0 /4** when no access group was applied to the **rp-address** command (refer to *rp-address <ip address> on page 4203*). Otherwise, it is the name of the access group.
state	Optional. Displays multicast route PIM state information.
traffic	Optional. Displays active PIM-SM control traffic statistics.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following is sample output from the **show ip pim-sparse** command:

```
>enable
#show ip pim-sparse
Global PIM Sparse Mode Settings
 Join/Prune interval: 60, SPT threshold: 1
```

The following is sample output from the **show ip pim-sparse interfaces** command:

```
>enable
#show ip pim-sparse interfaces
eth 0/1 is UP
  PIM Sparse
  DR: itself
  Local Address: 192.168.1.254
  Hello interval (sec): 30, Neighbor timeout (sec): 105
  Propagation delay (ms): 500, Override interval (ms): 2500

tunnel 1 is UP
  PIM Sparse
  DR: 172.16.1.10
  Local Address: 172.16.1.9
  Hello interval (sec): 30, Neighbor timeout (sec): 105
  Propagation delay (ms): 500, Override interval (ms): 2500

tunnel 2 is UP
  PIM Sparse
  DR: 172.16.2.10
  Local Address: 172.16.2.9
  Hello interval (sec): 30, Neighbor timeout (sec): 105
  Propagation delay (ms): 500, Override interval (ms): 2500
```

The following is sample output from the **show ip pim-sparse neighbor** command:

```
>enable
#show ip pim-sparse neighbor
```



```
Port          Neighbor        Holdtime(sec)   Age(sec)       Uptime(sec)
-------------------------------------------------------------------------------------------------
tunnel 1      172.16.1.10     105             19             241908
tunnel 2      172.16.2.10     105             23             241913
```

The following is sample output from the **show ip pim-sparse rp-map** command:

```
>enable
#show ip pim-sparse rp-map
Number of group-to-RP mappings: 5
Group address           RP address
-----------------------------------------------------
225.1.0.1               192.168.0.254
225.1.0.2               192.168.0.254
225.1.0.3               192.168.0.254
```

The following is sample output from the **show ip pim-sparse rp-set** command:

```
>enable
#show ip pim-sparse rp-set
Group address           Static-RP-address
-----------------------------------------------------------
224.0.0.0/4             192.168.0.254
MCAST_ACL_1             192.168.1.254
MCAST_ACL_2             192.168.2.254
MCAST_ACL_3             192.168.3.254
```

The following is sample output from the **show ip pim-sparse state** command:

```
>enable
#show ip pim-sparse state
PIM-SM State Table
Flags: S - Sparse, C - Connected, P - Pruned, J - Join SPT, T - SPT-bit Set,
F - Register, R - RP-bit Set
Timers: Uptime/Expires

(*, 225.1.0.1), 02:42:03/00:03:04, RP 192.168.0.254, Flags: SC
 Forwarding Entry: Yes
 Incoming interface: tunnel 2, RPF nbr 172.16.2.10
 Upstream Join/Prune State: Joined
 Register State: No Info
 RegStop Timer (sec): stopped
 Join/Prune Timer (sec): 57
 Override Timer (sec): stopped
 Multicast Border Router: 0.0.0.0
 Packets Forwarded: 2
```



```
 Outgoing interface list:
   eth 0/1, Forward, 02:42:03/00:03:03
     Downstream Join/Prune State: Join
     Assert Winner State: No Info
     Assert Timer (sec): stopped
     Assert Winner: 0.0.0.0
     Assert Winner Metric: infinity
     Local Membership: Yes
     Forwarding State: Forwarding
 Inherited output list:
   eth 0/1
```

The following is sample output from the **show ip pim-sparse traffic** command:

```
>enable
#show ip pim-sparse traffic
                    Rx        Tx        Rx                Tx
Port: eth 0/1
 Hello:             7         8334      J/P:        0     0
 Register:          0         0         RegStop:    0     0
 Assert:            0         0
Port: tunnel 1
 Hello:             8327      8333      J/P:        0     57
 Register:          0         0         RegStop:    0     0
 Assert:            0         0
Port: tunnel 2
 Hello:             8323      8334      J/P:        0     11949
 Register:          0         0         RegStop:    0     0
 Assert:            0         0
Total
 Hello:             16657     25001     J/P:        0     12006
 Register:          0         0         RegStop:    0     0
 Assert:            0         0
```

show ip policy

Use the **show ip policy** command to display the interfaces which have route maps configured. This command is used for troubleshooting policy-based routing.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip policy** command:

```
>enable
#show ip policy

Interface       Route-map
eth 0/1         ISP_A
eth 0/2         ISP_B
```


show ip policy-class

Use the **show ip policy-class** command to display the configured session limit and specific host IP addresses of all current sessions. Refer to *ip policy-class <ipv4 acp name> on page 1434* for information on configuring access policies.Variations of this command include:

show ip policy-class
show ip policy-class *<name>*
show ip policy-class host-sessions
show ip policy-class *<name>* **host-sessions**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

host-sessions	Optional. Displays specific host IP addresses of all current sessions.
<name>	Optional. Displays policy class information for a specific policy class.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 12.1	Command was expanded to include **host-sessions**.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip policy-class** command:

```
>enable
#show ip policy-class

Maximum policy-sessions: 17400
Policy-class “Private”:
 136 current sessions (5800 max)
 Entry 1 - allow list self self
 Entry 2 - nat source list wizard-ics interface ppp 1 overload
Policy-class “Public”:
 0 current sessions (5800 max)
```

The following is sample output from the **show ip policy-class host-sessions** command:

```
>enable
#show ip policy-class host-sessions

Policy-class “Private”:
 100 policy-sessions allowed per source address.

 Src IP Address   Sessions
 ---------------   --------
 192.168.1.100    1
 192.168.1.101    35
 192.168.1.121    100   (maximum allowed)

Policy-class “Public”:
 No limit for policy-sessions allowed per host.
```

The following is sample output from the **show ip policy-class** <*name*> **host-sessions** command for the policy class named **Private**:

```
>enable
#show ip policy-class Private host-sessions

Policy-class “Private”:
 100 policy-sessions allowed per source address.

 Src IP Address   Sessions
 ---------------   --------
 192.168.1.100    1
 192.168.1.101    35
 192.168.1.121    100   (maximum allowed)
```


show ip policy-sessions

Use the **show ip policy-sessions** command to display a list of current Internet Protocol version 4 (IPv4) access control policy (ACP) associations. Refer to *ip policy-class <ipv4 acp name> on page 1434* for information on configuring ACPs. Variations of this command include:

show ip policy-sessions
show ip policy-sessions *<ipv4 acp name>*
show ip policy-sessions *<ipv4 acp name>* **include-deleted**
show ip policy-sessions *<ipv4 acp name>* **timeline**
show ip policy-sessions any-vrf
show ip policy-sessions any-vrf include-deleted
show ip policy-sessions any-vrf timeline
show ip policy-sessions include-deleted
show ip policy-sessions pending
show ip policy-sessions timeline
show ip policy-sessions vrf *<name>*
show ip policy-sessions vrf *<name>* **include-deleted**
show ip policy-sessions vrf *<name>* **timeline**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv4 acp name>	Optional. Displays policy class associations for the specified IPv4 ACP.
include-deleted	Optional. Displays all IPv4 ACP firewall sessions, including active associations (through which the firewall is allowed to pass traffic), and associations flagged for deletion (through which the firewall is forbidden to pass traffic). Associations flagged for deletion will usually be freed within a few seconds of timeout or deletion, depending on packet congestion; servicing of packets is given priority. New traffic matching an association will create a new active association, provided the traffic still matches an ACP **allow** or network address translation (**NAT**) entry. (This parameter is only valid on the NetVanta 3200.)
timeline	Optional. Displays a timeline of IPv4 ACP firewall session creations and peak numbers of policy sessions per hour over the last 24 hours.
any-vrf	Optional. Displays information for all virtual routing and forwardings (VRFs), including the default.
pending	Optional. Displays any currently pending ACP sessions.

vrf <*name*>	Optional. Displays information only for the specified VRF. If a VRF is not specified, the default unnamed VRF is assumed.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command was expanded to include the **all** parameter.
Release 17.1	Command was expanded to include the parameters **vrf** and **include-deleted** (NetVanta 3200 only), as well as the modifiers **begin**, **exclude**, and **include**.
Release 17.5	Command was expanded to include the **timeline** parameter.
Release R10.1.0	Command was expanded to include the **pending** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **show ip policy-sessions** command, and displays information for IPv4 ACPs:

```
>enable
#show ip policy-sessions
Protocol (TTL) [in crypto map] -> [out crypto map] Dest VRF, Dest policy-class
 Src IP Address        Src Port        Dest IP Address    Dst Port   NAT IP Address    NAT Port
-------------------------------------------------------------------------------------------------------------------------------
Policy class “Public”:
tcp (13)
 192.168.1.142         2621            192.168.19.2       1          10.10.10.1        3000
tcp (13)
 192.168.1.142         2622            192.168.19.2       2          10.10.10.1        3001
tcp (13)
 192.168.1.142         2623            192.168.19.2       3          10.10.10.1        3002
```


The following is sample output from the **show ip policy-sessions include-deleted** command:

```
>enable
#show ip policy-sessions include-deleted

Src Vrf (if not default), Src policy class:

Protocol (TTL) [in crypto map] -> [out crypto map] Dest VRF, Dest policy-class
 Src IP Address       Src Port      Dest IP Address       Dst Port      NAT IP Address    NAT Port
-------------------------------------------------------------------------------------------------------------------------------------------
Policy class "Private":
Policy class “Private_Aqua”:
Policy class “Private_Black”:
Policy class “Private_Crimson”:
Policy class “Private_Green”:
Policy class “Private_Orange”:
Policy class “Private_Purple”:
Policy class “Private_Yellow”:
Policy class "Public":
Policy class "Public2":
Policy class "self":
udp (60) -> Public2
 10.22.160.134        1027          10.22.160.254         53
Policy class "default":
```

The following is sample output from the **show ip policy-sessions any-vrf include-deleted** command:

```
>enable
#show ip policy-sessions any-vrf include-deleted

Src Vrf (if not default), Src policy class:
Protocol (TTL) [in crypto map] -> [out crypto map] Dest VRF, Dest policy-class
Src IP Address       Src Port      Dest IP Address       Dst Port      NAT IP Address    NAT Port
-------------------------------------------------------------------------------------------------------------------------------------------
Policy class "Private":
Policy class "Public":
Policy class "self":
Policy class "default":
VRF "Green", Policy class "Private":
tcp (418) -> Black, Public
 192.168.121.2        35257         192.168.10.19         21      s     192.168.9.2         35257
tcp (593) -> Black, Public
 192.168.121.2        35333         192.168.10.19         20       s    192.168.9.2         2759
tcp (600) -> Black, Public
 192.168.121.2        65283         192.168.10.207        80      s     192.168.9.2         65283
tcp (4) -> Black, Public
 192.168.121.2        1606          192.168.10.209        80      s     192.168.9.2         1606
```



```
tcp (600) -> Black, Public
 192.168.121.2       3648        192.168.10.210      80     s     192.168.9.2         3648
tcp (502) -> Black, Public
 192.168.121.3       52429       192.168.10.19       21     s     192.168.9.2         52429
VRF "Green", Policy class "Public":
VRF "Green", Policy class "self":
VRF "Green", Policy class "default":
VRF "Black", Policy class "Private":
VRF "Black", Policy class "Public":
VRF "Black", Policy class "self":
VRF "Black", Policy class "default":
```

The following is sample output from the **show ip policy-sessions timeline** command:

```
#show ip policy-sessions timeline
Period: Feb 08 12:00 - Feb 09 12:00          Current Time: 09 Feb 2009 12:54:46

Hour     New      Peak
-------- -------- -------
12:00    13115    818
13:00    13810    769
14:00    13177    748
15:00    13373    753
16:00    14451    982
17:00    13555    831
18:00    13825    741
19:00    14130    827
20:00    13005    870
21:00    13640    803
22:00    13081    781
23:00    13893    799
00:00    13003    783
01:00    14077    937
02:00    13240    854
03:00    12448    803
04:00    12518    1018
05:00    12533    843
06:00    12818    752
07:00    16119    934
08:00    22813    996
09:00    20361    1041
10:00    28474    1221
11:00    20361    1454
```


#show ip policy-sessions pending

```
Protocol (TTL, [P]), ALG Name [Flags] [in crypto map] -> [out crypto map]
   (P - Persistent. Pending session is duplicated before being made active)
   (*  - Primary selector, compared when searching the pending session list)
   Src IP Address    Src Port   Dest IP Address   Dst Port   Policy Class [Selector 1]
   Src IP Address    Src Port   Dest IP Address   Dst Port   Policy Class [Selector 2]
   ---------------   --------   ---------------   --------   ------------
udp (53),    [0x20040C22 0x00000000]
  192.168.48.100     5738       10.22.11.33       0          PRIVATE
* 10.22.11.33        0          10.22.11.48       57388      PUBLIC
udp (60),   [0x20040C22 0x00000000]
  192.168.48.100     57388      10.22.11.33       0          PRIVATE
* 10.22.11.33        0          10.22.11.48       57388      PUBLIC
```

show ip policy-stats

Use the **show ip policy-stats** command to display a list of current Internet Protocol version 4 (IPv4) access control policy (ACP) statistics. Refer to *ip policy-class <ipv4 acp name> on page 1434* for information on configuring IPv4 ACPs. Variations of this command include:

show ip policy-stats
show ip policy-stats *<ipv4 acp name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv4 acp name>	Optional. Displays policy class statistics for a specific IPv4 ACP.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays a list of current IPv4 ACP statistics:

>enable
#show ip policy-stats

show ip prefix-list

Use the **show ip prefix-list** command to display Border Gateway Protocol (BGP) prefix list information. Variations of this command include:

show ip prefix-list <*name*>
show ip prefix-list detail <*name*>
show ip prefix-list summary <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*name*>	Shows information for a specific prefix list.
detail	Optional. Shows a listing of the prefix list rules and their hit counts.
summary	Optional. Shows information about the entire prefix list.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

If the **show ip prefix-list** command is issued with no arguments, a listing of the prefix-list rules, but no hit count statistics, is displayed.

Usage Examples

The following example displays information about the prefix list **test**.

```
>enable
#show ip prefix-list test
ip prefix-list test: 4 entries
   seq 5 permit 0.0.0.0/0 ge 8 le 8
   seq 10 deny 0.0.0.0/0 ge 9 le 9
   seq 15 permit 0.0.0.0/0 ge 10 le 10
   seq 20 deny 0.0.0.0/0 ge 11
```


show ip protocols

Use the **show ip protocols** command to display IP routing protocol parameters and statistics. Variations of this command include:

show ip protocols
show ip protocols vrf <*name*>

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

vrf <*name*>	Optional. Displays IP routing protocol parameters and statistics for the specified virtual routing and forwarding (VRF) instance. If no VRF is specified, statistics displayed are for the default (unnamed) VRF instance.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command was expanded to include the **vrf** <*name*> parameter.

Usage Examples

The following is sample output from the **show ip protocols** command:

```
>enable
#show ip protocols
Sending updates every 30 seconds, next due in 8 seconds
 Invalid after 180 seconds, hold down time is 120 seconds
 Redistributing: rip
 Default version control: send version 2, receive version 2
  Interface      Send Ver.      Rec Ver.
    eth 0/1          2              2
    ppp 1            2              2
 Routing for networks:
   1.1.1.0/24
```


show ip route

Use the **show ip route** command to display the contents of the Internet Protocol version 4 (IPv4) route table. Variations of this command include:

show ip route
show ip route *<ipv4 address>*
show ip route *<ipv4 address>* *<subnet mask>*
show ip route *<ipv4 address>* **longer-prefixes**
show ip route *<ipv4 address>* *<subnet mask>* **longer-prefixes**
show ip route bgp
show ip route bgp verbose
show ip route connected
show ip route ospf
show ip route ospf verbose
show ip route rip
show ip route rip verbose
show ip route static
show ip route static verbose
show ip route summary
show ip route summary realtime
show ip route table
show ip route vrf *<name>*
show ip route vrf *<name>* *<ipv4 address>*
show ip route vrf *<name>* *<ipv4 address>* *<subnet mask>*
show ip route vrf *<name>* *<ipv4 address>* **longer-prefixes**
show ip route vrf *<name>* *<ipv4 address>* *<subnet mask>* **longer-prefixes**
show ip route vrf *<name>* **bgp**
show ip route vrf *<name>* **connected**
show ip route vrf *<name>* **ospf**
show ip route vrf *<name>* **rip**
show ip route vrf *<name>* **static**
show ip route vrf *<name>* **summary**
show ip route vrf *<name>* **table**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<ipv4 address>	Optional. Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Optional. Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
bgp	Optional. Displays only the IPv4 routes associated with Border Gateway Protocol (BGP).
connected	Optional. Displays only the IPv4 routes for directly connected networks.
longer-prefixes	Optional. Displays only the IPv4 routes matching the specified network.
ospf	Optional. Displays only the IPv4 routes associated with Open Shortest Path First version 2 (OSPFv2).
rip	Optional. Displays only the IPv4 routes that were dynamically learned through Routing Information Protocol (RIP).
static	Optional. Displays only the IPv4 routes that were statically entered.
summary	Optional. Displays a summary of all IPv4 route information.
summary realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.
table	Optional. Displays a condensed version of the IPv4 route table.
verbose	Optional. Enables detailed messaging.
vrf *<name>*	Optional. Displays only the IPv4 routes for the specified virtual routing and forwarding (VRF).

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 16.1	Expanded to include the **vrf** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A1	Command was expanded to include the **verbose** parameter.
Release 17.2	Command was enhanced to show the best route to the given IP address and the **longer-prefixes** parameter was added.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example shows how to display IPv4 routes learned via BGP. The values in brackets after a BGP route entry represent the entry's administrative distance and metric:

```
>enable
#show ip route bgp
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
       IA - OSPF inter area, N1 - OSPF NSSA external type 1
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
       E2 - OSPF external type 2
Gateway of last resort is 10.15.43.17 to network 0.0.0.0
B    1.0.0.0/8 [30/0] via 10.15.43.17, fr 1.17
B    2.0.0.0/9 [30/0] via 10.15.43.17, fr 1.17
B    2.128.0.0/10 [30/0] via 10.15.43.17, fr 1.17
B    2.192.0.0/11 [30/0] via 10.15.43.17, fr 1.17
B    2.224.0.0/12 [30/0] via 10.15.43.17, fr 1.17
B    2.240.0.0/13 [30/0] via 10.15.43.17, fr 1.17
```

The following example shows output for the **show ip route vrf RED summary** command.

```
>enable
#show ip route vrf RED summary
Route Source    FIB       Local-RIB
Connected       16        16
Static          16        16
Other           31        31

Total           63        63
```


The following example shows how to display IPv4 routes learned in VRF **RED**. The values in brackets after a route entry represent the entry's administrative distance and metric:

```
>enable
#show ip route vrf RED
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
       IA - OSPF inter area, N1 - OSPF NSSA external type 1
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
       E2 - OSPF external type 2
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
S     0.0.0.0/0 [1/0] via 192.168.1.1, eth 0/2.301
C     192.168.1.0/24 is directly connected, eth 0/2.301
C     192.168.50.0/30 is directly connected, fr 1.16
C     192.168.50.1/32 is directly connected, fr 1.16
C     192.168.51.0/30 is directly connected, fr 2.16
C     192.168.54.0/30 is directly connected, ppp 1
C     192.168.55.0/30 is directly connected, hdlc 1
C     192.168.56.0/30 is directly connected, fr 11.16
S     192.168.101.0/24 [1/0] via 192.168.50.1, fr 1.16
S     192.168.102.0/24 [1/0] via 192.168.51.1, fr 2.16
S     192.168.106.0/24 [1/0] via 192.168.55.1, hdlc 1
S     192.168.107.0/24 [1/0] via 192.168.56.1, fr 11.16
S     192.168.109.0/24 [1/0] via 192.168.1.253, eth 0/2.301
```

The following example shows output for the **show ip route** command. The values in brackets after a route entry represent the entry's administrative distance and metric:

```
>enable
#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
       E1 - OSPF external type 1, E2 - OSPF external type 2
       IA - OSPF inter area

Gateway of last resort is 10.22.18.254 to network 0.0.0.0

S     0.0.0.0/0 [1/0] via 10.22.18.254, eth 0/1
S     10.22.16.0/24 [1/0] via 10.22.18.254, eth 0/1
S     10.22.17.0/24 [1/0] via 10.22.18.254, eth 0/1
C     10.22.18.0/24 is directly connected, eth 0/1
C     192.168.25.0/31 is directly connected, loop 1
C     192.168.26.1/32 is directly connected, loop 2
C     192.168.27.0/24 is directly connected, loop 3
C     192.168.249.0/24 is directly connected, eth 0/2
```


The following example shows output for the **show ip route** <*ipv4 address*> command. This data explains the resulting route a packet will be sent through.

>**enable**
#show ip route 10.22.16.16
Routing entry for 10.22.16.0/24
Known via “static”
Distance 1, metric 0, candidate default path
Routing Next Hop(s):
10.22.18.254, via eth 0/1
Route metric is 0

The following example shows output for the **show ip route** <*ipv4 address*> **longer-prefixes** command. Using the **longer-prefixes** parameter displays only the matching routes.

>**enable**
#show ip route 10.22.16.0 longer-prefixes
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
E1 - OSPF external type 1, E2 - OSPF external type 2
IA - OSPF inter area

Gateway of last resort is 10.22.18.254 to network 0.0.0.0

show ip route-cache express

Use the **show ip route-cache express** command to display the addresses currently being express cached in hardware. Variations of this command include:

show ip route-cache express
show ip route-cache express count

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

count	Optional. Displays only the total number of entries stored in the route cache.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following is sample output from the **show ip route-cache express** command:

```
>enable
#show ip route-cache express
DESTINATION     MASK              GATEWAY
-------------------------------------------------------------------------------
199.0.50.2      255.255.255.255   10.100.43.251
199.0.45.2      255.255.255.255   10.100.43.251
198.110.47.2    255.255.255.255   10.100.43.251
198.50.42.2     255.255.255.255   10.100.43.251
198.0.46.2      255.255.255.255   10.100.43.251
198.0.41.2      255.255.255.255   10.100.43.251
```

The following is sample output from the **show ip route-cache express count** command:

```
>enable
#show ip route-cache express count
Total number of express routes: 26
```


show ip route-cache express host-table

Use the **show ip route-cache express host-table** command to display the hardware host entries currently used to route packets to directly connected networks in Layer 3 switching. Variations of this command include:

show ip route-cache express host-table
show ip route-cache express host-table count

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

count	Optional. Specifies the output is limited to the number of entries stored in the Address Resolution Protocol (ARP) table.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following is sample output from the **show ip route-cache express host-table** command:

```
>enable
#show ip route-cache express host-table
DESTINATION     MAC ADDRESS        INTERFACE
-------------------------------------------------------------------------------
10.23.131.254   00:A0:C8:00:7E:D3  vlan 1
20.1.1.2        00:DE:AD:00:55:55  vlan 20
21.1.1.2        00:A0:C8:00:78:A8  vlan 21
22.1.1.2        00:A0:C8:24:7E:6A  vlan 22
```

show ip security

Use the **show ip security** command to display a list of threats with descriptions, corresponding IDs, default weights, and current weights. Variations of this command include:

show ip security any-vrf blocked-traffic timeline
show ip security any-vrf threats
show ip security any-vrf threats <*id*>
show ip security any-vrf threats <*id*> **realtime**
show ip security any-vrf threats realtime
show ip security any-vrf threats sort-by first-observed
show ip security any-vrf threats sort-by first-observed realtime
show ip security any-vrf threats sort-by hits
show ip security any-vrf threats sort-by hits realtime
show ip security any-vrf threats sort-by id
show ip security any-vrf threats sort-by id realtime
show ip security any-vrf threats sort-by last-observed
show ip security any-vrf threats sort-by last-observed realtime
show ip security any-vrf threats sort-by weight
show ip security any-vrf threats sort-by weight realtime
show ip security blocked-traffic timeline
show ip security threats
show ip security threats <*id*>
show ip security threats <*id*> **realtime**
show ip security threats realtime
show ip security threats sort-by first-observed
show ip security threats sort-by first-observed realtime
show ip security threats sort-by hits
show ip security threats sort-by hits realtime
show ip security threats sort-by id
show ip security threats sort-by id realtime
show ip security threats sort-by last-observed
show ip security threats sort-by last-observed realtime
show ip security threats sort-by weight
show ip security threats sort-by weight realtime
show ip security vrf <*name*> **blocked-traffic timeline**
show ip security vrf <*name*> **threats**
show ip security vrf <*name*> **threats** <*id*>
show ip security vrf <*name*> **threats** <*id*> **realtime**
show ip security vrf <*name*> **threats realtime**
show ip security vrf <*name*> **threats sort-by first-observed**
show ip security vrf <*name*> **threats sort-by first-observed realtime**
show ip security vrf <*name*> **threats sort-by hits**
show ip security vrf <*name*> **threats sort-by hits realtime**
show ip security vrf <*name*> **threats sort-by id**
show ip security vrf <*name*> **threats sort-by id realtime**

show ip security vrf <*name*> **threats sort-by last-observed**
show ip security vrf <*name*> **threats sort-by last-observed realtime**
show ip security vrf <*name*> **threats sort-by weight**
show ip security vrf <*name*> **threats sort-by weight realtime**

Syntax Description

any-vrf	Optional. Displays every available virtual routing and forwarding (VRF) on the device.
blocked-traffic timeline	Optional. Displays an hour-by-hour count of blocked threats and policy discards.
first-observed	Optional. Sorts the threat list by the first-observed threat.
hits	Optional. Sorts the threat list by number of hits.
id	Optional. Sorts the threat list by threat ID.
<*id*>	Optional. Displays a specific threat as identified by its threat ID.
last-observed	Optional. Sorts the threat list by the last-observed threat.
realtime	Optional. Lists the threats as they occur in real time rather than historical threat data.
sort-by <*option*>	Optional. Defines the criteria, by <*option*>, by which the threat list will be sorted. If **sort-by** is not indicated, the list will be sorted using the descending order of hits. All options will be sorted in descending order with the exception of threat IDs.
threats	Optional. Displays all observed security threats.
vrf <*name*>	Optional. Displays a specified named VRF.
weight	Optional. Sorts the threat list by threat weight.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Functional Notes

The **show ip security** command displays a list of threats with descriptions, corresponding IDs, default weights, and current weights. For threats that have been observed the number of hits, the time it was first observed, and the time it was most recently observed is displayed. Threat lists are sorted by hits unless another option is chosen by the user. All sorting options are displayed in descending order except for threat IDs. A single ID can be specified to display only that threat's information. The unnamed default VRF is implied unless a named VRF or **any-vrf** is specified. Historical data is displayed unless **realtime** is specified. Threats that have been blocked on the default unnamed VRF or **any-vrf** can also be viewed using **blocked-traffic timeline**.

Usage Examples

The following example displays a list of all threats on the default unnamed VRF sorted by threat weight:

>**enable**
#show ip security threats sort-by weight

The following example displays an hour-by-hour count of all blocked threats on the named VRF **MyVRF**:

>**enable**
#show ip security vrf MyVRF blocked-traffic timeline

show ip traffic

Use the **show ip traffic** command to display all Internet Protocol version 4 (IPv4) traffic statistics. Variations of this command include:

show ip traffic
show ip traffic netstat
show ip traffic realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

netstat	Optional. Displays active IPv4 Transmission Control Protocol (TCP) connections.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.5	Command was expanded to include the **netstat** keyword.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example displays all IPv4 traffic statistics:

>**enable**
#show ip traffic

IP statistics:
Routing discards: 0
Rcvd: 15873 total, 7617 delivered
0 header errors, 0 address errors
0 unknown protocol, 0 discards
0 checksum errors, 0 bad hop counts
Sent: 8281 generated, 4459 forwarded
0 no routes, 0 discards
Frags: 0 reassemble required, 0 reassembled, 0 couldn't reassemble
0 created, 0 fragmented, 0 couldn't fragment

UDP statistics:
Rcvd: 3822 total, 0 checksum errors, 0 no port
Sent: 3822 total

TCP statistics:
Retrans Timeout Algorithm: 0
Min retrans timeout (ms): 0
Max retrans timeout (ms): 0
Max TCP Connections: 0
0 active opens, 64 passive opens, 0 failed attempts
5 establish resets, 1 establish current
3795 segments received, 4459 segments sent, 26 segments retransmitted

show ip urlfilter

Use the **show ip urlfilter** command to display configured uniform resource locator (URL) filter and server information.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip urlfilter** command:

```
>enable
#show ip urlfilter

Configured for Websense URL filtering.
Filters
-------
Name: “filter1”
Ports: HTTP(80)
Interfaces that filter is applied to:
eth 0/2 inbound
Servers
-------
IP address: 10.100.23.116
Port: 15868
Timeout: 5
Excluded domains
----------------
Permit www.adtran.com
Other Settings
```


show ip urlfilter exclusive-domain

Use the **show ip urlfilter exclusive-domain** command to display all configured domains excluded (either always allowed or always blocked) from uniform resource locator (URL) filtering.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip urlfilter exclusive-domain** command:

```
>enable
#show ip urlfilter exclusive-domain

Excluded domains
----------
Permit www.adtran.com
```


show ip urlfilter statistics

Use the **show ip urlfilter statistics** command to display statistics for uniform resource locator (URL) filter requests and responses.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show ip urlfilter statistics** command:

```
>enable
#show ip urlfilter statistics

Current outstanding requests to filter server: 0
Current response packets buffered from web server: 2
Max outstanding requests to filter server: 3
Max response packets buffered from web server: 5
Total requests sent to filter server: 400
Total responses received from filter server: 400
Total requests allowed: 398
Total requests blocked: 2
```


show ip urlfilter top-websites

Use the **show ip urlfilter top-websites** command to display configured uniform resource locator (URL) filter and top websites reporting information. Variations of this command include the following:

show ip urlfilter top-websites
show ip urlfilter top-websites *<number>*
show ip urlfilter top-websites all
show ip urlfilter top-websites all *<number>*
show ip urlfilter top-websites daily
show ip urlfilter top-websites daily *<number>*
show ip urlfilter top-websites hourly
show ip urlfilter top-websites hourly *<number>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

all	Optional. Specifies that top websites statistics for all lists will be displayed.
daily	Optional. Specifies that top websites statistics in daily increments will be displayed.
hourly	Optional. Specifies that top websites statistics in hourly increments will be displayed.
<number>	Optional. Specifies how many websites to show on the report. Range is **5** to **20** websites.

Default Values

By default, a 15-minute incremented list of the 10 top websites requests is shown.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

The top websites statistic lists show the previous interval, not the current one. The output shows the period for which the statistics were collected, as well as the current time so it can be determined when the next update will occur.

Usage Examples

The following example displays the top 5 websites visited in the last 15 minutes:

#show ip urlfilter top-websites 5

Top Websites Visited
Period: Apr 26 08:55:00--Apr 26 09:10:00 Current Time: 09:15:34
Allow mode: enabled
The visits listed below are visits which were permitted. These statistics do not include websites explicitly filtered using exclusive domains.

Domain Name	Visits	Last Visitor	Visit Time
www.gmail.com	767	10.22.160.7	Apr 26 08:55:47
www.google.com	540	10.22.160.88	Apr 26 09:05:27
www.adtran.com	67	10.22.160.107	Apr 26 08:59:16
www.cisco.com	67	10.22.160.5	Apr 26 09:01:05
www.partypoker.com	15	10.22.160.45	Apr 26 09:04:43

show ipv6 access-list

Use the **show ipv6 access-list** command to display all configured Internet Protocol version 6 (IPv6) access control lists (ACLs) in the system. Variations of this command include:

show ipv6 access-list
show ipv6 access-list *<ipv6 acl name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv6 acl name>	Optional. Specifies a particular IPv6 ACL to display.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Functional Notes

The **show ipv6 access-list** command displays all configured IPv6 ACLs in the system. All entries in the IPv6 ACL are displayed, and a counter indicating the number of packets matching the entry is listed.

Usage Examples

The following is sample output from the **show ipv6 access-list** command, and displays information for the IPv6 ACL **Privatev6**:

```
>enable
#show ipv6 access-list Privatev6
Extended IPv6 access-list Privatev6
    deny tcp any eq telnet any (0 matches)
    deny tcp any any eq telnet (0 matches)
    permit ipv6 any host 2000:1::1 (0 matches)
    permit ipv6 host 2000:2::1 any (0 matches)
    permit icmpv6 any any (0 matches)
```


show ipv6 cache

Use the **show ipv6 cache** command to display the contents of the Internet Protocol version 6 (IPv6) route cache for each interface in a given virtual private network (VPN) routing and forwarding (VRF) instance. The route cache contains information about which egress interface, IPv6 gateway address, and MAC address to use when forwarding packets to a given destination. Variations of this command include:

show ipv6 cache
show ipv6 cache vrf <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

vrf <*name*>	Optional. Specifies a nondefault VRF instance for which to display route cache information. If no VRF instance is specified, route cache information for the default VRF instance is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 18.3	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example displays route cache statistics for the default VRF instance:

>**enable**
#show ipv6 cache
INGRESS: giga-eth 0/1.1001
DEST: 2001:1111:2222:3333:4444:5555:6666:7777, EGRESS: giga-eth 0/1.1002,
COUNT: 1000000000, GATEWAY: 2001:1111:2222:3333:4444:5555:6666:0001,
MAC: 00:a0:c8:00:00:01, ID: 0x01000000
DEST: 2001::1, EGRESS: ppp 1,
COUNT: 100, GATEWAY: 2001::1:0001,
MAC: n/a, ID: 0x01010000
DEST: 2001::2, EGRESS: ppp 1,
COUNT: 100, GATEWAY: 2001::1:0001,
MAC: n/a, ID: 0x01020000

show ipv6 crypto ipsec sa

Use the **show ipv6 crypto ipsec sa** command to display information about the Internet Protocol version 6 (IPv6) cryptographic subsystem and IP security (IPsec) security association (SA) configuration on the AOS device. Variations of this command include:

show ipv6 crypto any-vrf ipsec sa
show ipv6 crypto any-vrf ipsec sa map *<name>*
show ipv6 crypto any-vrf ipsec sa map *<name>* **inbound**
show ipv6 crypto any-vrf ipsec sa map *<name>* **outbound**
show ipv6 crypto any-vrf ipsec sa address *<ipv6 address>*
show ipv6 crypto any-vrf ipsec sa address *<ipv6 address>* **inbound**
show ipv6 crypto any-vrf ipsec sa address *<ipv6 address>* **outbound**
show ipv6 crypto any-vrf ipsec sa brief
show ipv6 crypto any-vrf ipsec sa brief inbound
show ipv6 crypto any-vrf ipsec sa brief outbound
show ipv6 crypto any-vrf ipsec sa inbound
show ipv6 crypto any-vrf ipsec sa internal-id *<id>*
show ipv6 crypto any-vrf ipsec sa internal-id *<id>* **inbound**
show ipv6 crypto any-vrf ipsec sa internal-id *<id>* **outbound**
show ipv6 crypto any-vrf ipsec sa ospfv3
show ipv6 crypto any-vrf ipsec sa ospfv3 inbound
show ipv6 crypto any-vrf ipsec sa ospfv3 outbound
show ipv6 crypto any-vrf ipsec sa outbound
show ipv6 crypto ipsec sa
show ipv6 crypto ipsec sa map *<name>*
show ipv6 crypto ipsec sa map *<name>* **inbound**
show ipv6 crypto ipsec sa map *<name>* **outbound**
show ipv6 crypto ipsec sa address *<ipv6 address>*
show ipv6 crypto ipsec sa address *<ipv6 address>* **inbound**
show ipv6 crypto ipsec sa address *<ipv6 address>* **outbound**
show ipv6 crypto ipsec sa brief
show ipv6 crypto ipsec sa brief inbound
show ipv6 crypto ipsec sa brief outbound
show ipv6 crypto ipsec sa inbound
show ipv6 crypto ipsec sa internal-id *<id>*
show ipv6 crypto ipsec sa internal-id *<id>* **inbound**
show ipv6 crypto ipsec sa internal-id *<id>* **outbound**
show ipv6 crypto ipsec sa ospfv3
show ipv6 crypto ipsec sa ospfv3 inbound
show ipv6 crypto ipsec sa ospfv3 outbound
show ipv6 crypto ipsec sa outbound
show ipv6 crypto vrf *<name>* **ipsec sa**
show ipv6 crypto vrf *<name>* **ipsec sa map** *<name>*
show ipv6 crypto vrf *<name>* **ipsec sa map** *<name>* **inbound**
show ipv6 crypto vrf *<name>* **ipsec sa map** *<name>* **outbound**

show ipv6 crypto vrf <*name*> **ipsec sa address** <*ipv6 address*>
show ipv6 crypto vrf <*name*> **ipsec sa address** <*ipv6 address*> **inbound**
show ipv6 crypto vrf <*name*> **ipsec sa address** <*ipv6 address*> **outbound**
show ipv6 crypto vrf <*name*> **ipsec sa brief**
show ipv6 crypto vrf <*name*> **ipsec sa brief inbound**
show ipv6 crypto vrf <*name*> **ipsec sa brief outbound**
show ipv6 crypto vrf <*name*> **ipsec sa inbound**
show ipv6 crypto vrf <*name*> **ipsec sa internal-id** <*id*>
show ipv6 crypto vrf <*name*> **ipsec sa internal-id** <*id*> **inbound**
show ipv6 crypto vrf <*name*> **ipsec sa internal-id** <*id*> **outbound**
show ipv6 crypto vrf <*name*> **ipsec sa ospfv3**
show ipv6 crypto vrf <*name*> **ipsec sa ospfv3 inbound**
show ipv6 crypto vrf <*name*> **ipsec sa ospfv3 outbound**
show ipv6 crypto vrf <*name*> **ipsec sa outbound**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

any-vrf	Optional. Displays IPsec information for all virtual routing and forwarding (VRF) instances.
vrf <*name*>	Optional. Displays IPsec information for a nondefault VRF instance.
map <*name*>	Optional. Displays IPsec security associations (SAs) created by the specified crypto map.
address <*ipv6 address*>	Optional. Displays all IPsec SAs associated with the designated peer IPv6 address. IPv6 addresses should be expressed in colon hexadecimal notation (**X:X:X:X::X**). For example, **2001:DB8:1::1**..
brief	Optional. Displays a brief listing of IPsec SAs.
inbound	Optional. Displays inbound IPsec SAs only.
outbound	Optional. Displays outbound IPsec SAs only.
internal-id <*id*>	Optional. Displays the IPsec SA with a specified internal ID. Valid range is **0** to **4294967295**.
ospfv3	Optional. Displays IPsec SAs created for Open Shortest Path First version 3 (OSPFv3) authentication and confidentiality.

Default Values

No default values are necessary for this command.

Command History

Release R10.5	Command was introduced.
Release R10.7	Command was expanded to include the **map** <*name*> parameter.

Usage Examples

The following is sample output from the **show ipv6 crypto ipsec sa ospfv3** command:

```
>enable
#show ipv6 crypto ipsec sa ospfv3
Peer IP Address: ::
  Direction: Inbound
  Encapsulation: ESP transport
  SPI: 0x00000BB8 (3000)
  RX Bytes: 512

Peer IP Address: ::
  Direction: Outbound
  Encapsulation: ESP transport
  SPI: 0x00000BB8 (3000)
  TX Bytes: 512
```

show ipv6 dhcp

Use the **show ipv6 dhcp** command to display the Dynamic Host Control Protocol version 6 (DHCPv6) Unique Identifier (DUID) of the AOS device. The DUID is used to identify the entire DHCPv6 client device independent of its interfaces and hardware.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example displays output from the **show ipv6 dhcp** command:

```
>enable
#show ipv6 dhcp
The DHCPv6 unique identifier (DUID) of this device is: 0003000100A0C800611F
```


show ipv6 dhcp binding

Use the **show ipv6 dhcp binding** command to display details about stateful information assigned and bound to individual Dynamic Host Control Protocol version 6 (DHCPv6) clients as maintained by the DHCPv6 server. Variations of this command include:

show ipv6 dhcp binding
show ipv6 dhcp binding *<ipv6 address>*
show ipv6 dhcp binding *<ipv6 address>* **summary**
show ipv6 dhcp binding summary
show ipv6 dhcp binding vrf *<name>*
show ipv6 dhcp binding vrf *<name> <ipv6 address>*
show ipv6 dhcp binding vrf *<name> <ipv6 address>* **summary**
show ipv6 dhcp binding vrf *<name>* **summary**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv6 address>	Optional. Limits the output to a single DHCPv6 client IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (for example, **2001:DB8:1::1**.
summary	Optional. Summarizes the command output.
vrf *<name>*	Optional. Limits output to a nondefault virtual routing and forwarding (VRF) instance. If no VRF is specified, bindings on all VRF instances are displayed.

Default Values

No default values necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example displays all DHCPv6 binding information:

```
>enable
#show ipv6 dhcp binding
Client: FE80::20F:35FF:FE2E:2AB9 eth 0/2
        DUID: 00030001000F352E2AB9
        Hostname: <unassigned>
        IA PD: IA ID 0x001A0001, T1 302400, T2 483840
                Prefix: 55:44:33:22::/64
                        preferred lifetime 604800, valid lifetime 2592000
                        expires as 2011/11/23 AD at 13:05:40 CST (56 seconds)
                Prefix: 44:33:22:11::/64
                        preferred lifetime 604800, valid lifetime 2592000
                        expires at 2011.11.23 AD at 13:05:40 CST (56 seconds)
        IA NA: IA ID 0x00000001, T1 43200, T2 69120
                Address: 2000:3::790DC94:6C36:9562 from pool MYPOOL
                        preferred lifetime 96400, valid lifetime 172800
                        expires at 2011.11.23 AD at 13:05:40 (56 seconds)
        IA NA: IA ID 0x00000002, T1 43200, T2 69120
                Address: 2000:3::4469:960:7C0E:EE6F
                        preferred lifetime 86400, valid lifetime 172800
                        expires at 2011.11.23 AD at 13:05:40 CST (56 seconds)
```

show ipv6 dhcp conflict

Use the **show ipv6 dhcp conflict** command to display detailed information about any addresses deemed as conflicting by a Dynamic Host Control Protocol version 6 (DHCPv6) client or by the DHCPv6 server when the client is pinged. Variations of this command include:

show ipv6 dhcp conflict
show ipv6 dhcp conflict *<ipv6 address>*
show ipv6 dhcp conflict vrf *<name>*
show ipv6 dhcp conflict vrf *<name> <ipv6 address>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv6 address>	Optional. Limits the output to conflicting addresses for the specified client address. IPv6 addresses should be expressed in colon hexadecimal format (for example, **2001:DB8:1::1**).
vrf *<name>*	Optional. Limits the output to a nondefault virtual routing and forwarding (VRF) instance. If no VRF is specified, conflicting addresses on all VRF instances are displayed.

Default Values

No default values necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example displays all DHCPv6 conflicting IPv6 addresses:

```
>enable
#show ipv6 dhcp conflict
Address/Prefix                          Reason      TTL (seconds)
1111:2222:333:4444:5555:66:7777/128     PING        44
1111:2222:333:4444:5555:66:7777/128     DECL        56
```


show ipv6 dhcp interface

Use the **show ipv6 dhcp interface** command to display the Dynamic Host Control Protocol version 6 (DHCPv6) mode and settings for interfaces configured for DHCPv6. Variations of this command include:

show ipv6 dhcp interface *<interface>*
show ipv6 dhcp interface *<interface>* **summary**
show ipv6 dhcp interface efm-group *<group id>*
show ipv6 dhcp interface mef-ethernet <*slot/port***>**
show ipv6 dhcp interface system-control-evc
show ipv6 dhcp interface system-control-evc summary
show ipv6 dhcp interface system-management-evc
show ipv6 dhcp interface system-management-evc summary

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Specifies the interface for which to display DHCPv6 settings. Specify interfaces in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id>*. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. Enter **show ipv6 dhcp interface ?** for a list of available interfaces.
efm-group *<group id>*	Specifies an Ethernet in the first mile (EFM) group ID. Range is **1** to **1024**.
mef-ethernet *<slot/port>*	Optional. Displays RapidRoute entries for the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Specifies DHCPv6 settings for the system control Ethernet virtual connection (EVC) are displayed.
system-management-evc	Specifies DHCPv6 settings for the system management EVC are displayed.
summary	Optional. Summarizes the command output.

Default Values

No default values necessary for this command.

Command History

Release R10.1.0	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.

Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.3.0	Command was expanded to include the Ethernet in the first mile (EFM) group interface.

Usage Examples

The following example displays the DHCPv6 mode and settings for the **eth 0/1** interface:

```
>enable
#show ipv6 dhcp interface eth 0/1
!
interface Ethernet 0/1
        ipv6
        ipv6 nd ra suppress
        ipv6 address dhcp
        ipv6 dhcp client pd prefix1
```

show ipv6 dhcp pool

Use the **show ipv6 dhcp pool** command to display the information about each configured Dynamic Host Control Protocol version 6 (DHCPv6) pool and the general statistics of the current pool assignments. Variations of this command include:

show ipv6 dhcp pool
show ipv6 dhcp pool *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Optional. Limits the command output to only the statistics for the specified DHCPv6 server pool.

Default Values

No default values necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example displays the configuration of all DHCPv6 server pools:

```
>enable
#show ipv6 dhcp pool
Pool POOL
        Link Addresses:
                22::/64
                22::/96
        Client Identifiers:
                112233445566 2
                112233445566
        Address Prefixes:
                22::/64 lifetime 60 30
        Host client-identifier AABBCCDD
                Hostname: server1
```



```
        Host client-identifier AABBCCDD1122
                Hostname: AACCDDBB
                Address: 22::99
Client: FE80::204:E2FF:FE3E:C786 eth 0/2
        DUID: 00000000000000000000000000DF
        Hostname: winxp
        IA NA: IA ID 0x00000001, T1 15, T2 24
                Address: 22::19C1:AC2:8277:CB39 from pool POOL
                        preferred lifetime 30, valid lifetime 60
                        expires at 2011.11.23 AD at 13:33: CST (47 seconds)
Client: FE80::B098:1B0E:27CA:A8AB eth 0/2
        DUID: 000100010D86F190019B9324A8E
        Hostname: <unassigned>
        IA NA: IA ID 0x0E000475, T1 15, T2 24
                Address: 22::4CC2:9F4E:3C68:1E55 from pool POOL
                        preferred lifetime 30, valid lifetime 60
                        expires at 2011.11.23 AD at 13:33:04 CST (46 seconds)
```


show ipv6 ffe

Use the **show ipv6 ffe** command to display current Internet Protocol version 6 (IPv6) RapidRoute fast forwarding engine (FFE) entries. Variations of this command include:

show ipv6 ffe

show ipv6 ffe destination <*ipv6 address*>
show ipv6 ffe destination <*ipv6 address*> **egress** <*interface*>
show ipv6 ffe destination <*ipv6 address*> **egress system-control-evc**
show ipv6 ffe destination <*ipv6 address*> **egress system-management-evc**

show ipv6 ffe destination <*ipv6 address*> **ingress** <*interface*>
show ipv6 ffe destination <*ipv6 address*> **ingress system-control-evc**
show ipv6 ffe destination <*ipv6 address*> **ingress system-management-evc**

show ipv6 ffe destination-port <*port*>
show ipv6 ffe destination-port <*port*> **egress** <*interface*>
show ipv6 ffe destination-port <*port*> **egress system-control-evc**
show ipv6 ffe destination-port <*port*> **egress system-management-evc**

show ipv6 ffe destination-port <*port*> **ingress** <*interface*>
show ipv6 ffe destination-port <*port*> **ingress system-control-evc**
show ipv6 ffe destination-port <*port*> **ingress system-management-evc**

show ipv6 ffe details
show ipv6 ffe details egress <*interface*>
show ipv6 ffe details egress system-control-evc
show ipv6 ffe details egress system-management-evc

show ipv6 ffe details ingress <*interface*>
show ipv6 ffe details ingress system-control-evc
show ipv6 ffe details ingress system-management-evc

show ipv6 ffe egress <*interface*>
show ipv6 ffe egress <*interface*> **destination** <*ipv6 address*>
show ipv6 ffe egress <*interface*> **destination-port** <*port*>
show ipv6 ffe egress <*interface*> **details**
show ipv6 ffe egress <*interface*> **icmp-type** <*type*>
show ipv6 ffe egress <*interface*> **protocol** <*protocol*>
show ipv6 ffe egress <*interface*> **source** <*ipv6 address*>
show ipv6 ffe egress <*interface*> **source-port** <*port*>
show ipv6 ffe egress <*interface*> **type** <*type*>
show ipv6 ffe egress ipsec <*rapidroute interface ID*>

show ipv6 ffe egress system-control-evc destination <*ipv6 address*>

show ipv6 ffe egress system-control-evc destination-port *<port>*
show ipv6 ffe egress system-control-evc details
show ipv6 ffe egress system-control-evc icmp-type *<type>*
show ipv6 ffe egress system-control-evc protocol *<protocol>*
show ipv6 ffe egress system-control-evc source *<ipv6 address>*
show ipv6 ffe egress system-control-evc source-port *<port>*
show ipv6 ffe egress system-control-evc type *<type>*

show ipv6 ffe egress system-management-evc destination *<ipv6 address>*
show ipv6 ffe egress system-management-evc destination-port *<port>*
show ipv6 ffe egress system-management-evc details
show ipv6 ffe egress system-management-evc icmp-type *<type>*
show ipv6 ffe egress system-management-evc protocol *<protocol>*
show ipv6 ffe egress system-management-evc source *<ipv6 address>*
show ipv6 ffe egress system-management-evc source-port *<port>*
show ipv6 ffe egress system-management-evc type *<type>*

show ipv6 ffe icmp-type *<type>*
show ipv6 ffe icmp-type *<type>* **egress** *<interface>*
show ipv6 ffe icmp-type *<type>* **egress system-control-evc**
show ipv6 ffe icmp-type *<type>* **egress system-management-evc**

show ipv6 ffe icmp-type *<type>* **ingress** *<interface>*
show ipv6 ffe icmp-type *<type>* **ingress system-control-evc**
show ipv6 ffe icmp-type *<type>* **ingress system-management-evc**

show ipv6 ffe ingress *<interface>*
show ipv6 ffe ingress *<interface>* **destination** *<ipv6 address>*
show ipv6 ffe ingress *<interface>* **destination-port** *<port>*
show ipv6 ffe ingress *<interface>* **details**
show ipv6 ffe ingress *<interface>* **icmp-type** *<type>*
show ipv6 ffe ingress *<interface>* **protocol** *<protocol>*
show ipv6 ffe ingress *<interface>* **source** *<ipv6 address>*
show ipv6 ffe ingress *<interface>* **source-port** *<port>*
show ipv6 ffe ingress *<interface>* **type** *<type>*
show ipv6 ffe ingress ipsec *<rapidroute interface ID>*

show ipv6 ffe ingress system-control-evc destination *<ipv6 address>*
show ipv6 ffe ingress system-control-evc destination-port *<port>*
show ipv6 ffe ingress system-control-evc details
show ipv6 ffe ingress system-control-evc icmp-type *<type>*
show ipv6 ffe ingress system-control-evc protocol *<protocol>*
show ipv6 ffe ingress system-control-evc source *<ipv6 address>*
show ipv6 ffe ingress system-control-evc source-port *<port>*
show ipv6 ffe ingress system-control-evc type *<type>*

show ipv6 ffe ingress system-management-evc destination <*ipv6 address*>
show ipv6 ffe ingress system-management-evc destination-port <*port*>
show ipv6 ffe ingress system-management-evc details
show ipv6 ffe ingress system-management-evc icmp-type <*type*>
show ipv6 ffe ingress system-management-evc protocol <*protocol*>
show ipv6 ffe ingress system-management-evc source <*ipv6 address*>
show ipv6 ffe ingress system-management-evc source-port <*port*>
show ipv6 ffe ingress system-management-evc type <*type*>

show ipv6 ffe peak
show ipv6 ffe peak history

show ipv6 ffe protocol <*protocol*>
show ipv6 ffe protocol <*protocol*> **egress** <*interface*>
show ipv6 ffe protocol <*protocol*> **egress system-control-evc**
show ipv6 ffe protocol <*protocol*> **egress system-management-evc**

show ipv6 ffe protocol <*protocol*> **ingress** <*interface*>
show ipv6 ffe protocol <*protocol*> **ingress system-control-evc**
show ipv6 ffe protocol <*protocol*> **ingress system-management-evc**

show ipv6 ffe source <*ipv6 address*>
show ipv6 ffe source <*ipv6 address*> **egress** <*interface*>
show ipv6 ffe source <*ipv6 address*> **egress system-control-evc**
show ipv6 ffe source <*ipv6 address*> **egress system-management-evc**

show ipv6 ffe source <*ipv6 address*> **ingress** <*interface*>
show ipv6 ffe source <*ipv6 address*> **ingress system-control-evc**
show ipv6 ffe source <*ipv6 address*> **ingress system-management-evc**

show ipv6 ffe source-port <*port*>
show ipv6 ffe source-port <*port*> **egress** <*interface*>
show ipv6 ffe source-port <*port*> **egress system-control-evc**
show ipv6 ffe source-port <*port*> **egress system-management-evc**

show ipv6 ffe source-port <*port*> **ingress** <*interface*>
show ipv6 ffe source-port <*port*> **ingress system-control-evc**
show ipv6 ffe source-port <*port*> **ingress system-management-evc**

show ipv6 ffe type <*type*>
show ipv6 ffe type <*type*> **egress** <*interface*>
show ipv6 ffe type <*type*> **egress system-control-evc**
show ipv6 ffe type <*type*> **egress system-management-evc**

show ipv6 ffe type <*type*> **ingress** <*interface*>
show ipv6 ffe type <*type*> **ingress system-control-evc**
show ipv6 ffe type <*type*> **ingress system-management-evc**

show ipv6 ffe wildcard
show ipv6 ffe wildcard system-control-evc
show ipv6 ffe wildcard system-management-evc
show ipv6 ffe wildcard interface <*interface*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

destination <*ipv6 address*>	Optional. Filters output by a destination IPv6 address. IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).
destination-port <*port*>	Optional. Filters output by destination Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port. Ports range from **0** to **65535**.
details	Optional. Displays detailed information. Refer to the Functional Notes for more information about using the details keyword.
egress <*interface*>	Optional. Displays RapidRoute entries for an egress interface. Specify an interface in the format <*interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | group id]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an EFM group interface use **efm-group 1**. Type **show ipv6 ffe egress ?** for a complete list of valid interfaces.
egress ipsec <*rapidroute interface ID*>	Optional. Displays RapidRoute entries that come from an Internet Protocol security (IPsec) security association (SA) on a specified RapidRoute interface. RapidRoute interface identifiers range from **1** to **16777215**.
icmp-type <*type*>	Optional. Displays RapidRoute entries using a specific Internet Control Message Protocol (ICMP) type. There are three types of ICMP to choose from: **echo** Displays ICMP echo RapidRoute entries. **reply** Displays ICMP reply RapidRoute entries. **0** to **255** Displays other ICMP types.

ingress <*interface*>	Optional. Displays RapidRoute entries for an ingress interface. Specify an interface in the format <*interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | group id]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an EFM group interface use **efm-group 1**. Type **show ipv6 ffe ingress ?** for a complete list of valid interfaces.
ingress ipsec <*rapidroute interface ID*>	Optional. Displays RapidRoute entries that go to an IPsec SA on a specified RapidRoute interface. RapidRoute interface identifiers range from **1** to **16777215**.
peak	Optional. Displays the current and peak count of RapidRoute sessions. Information is displayed for each eligible interface and the global values.
history	Optional. Displays a graphical presentation of the peak global RapidRoute cont per second for the last 60 seconds. Additionally displays the peak and average global RapidRoute count per minute for the last 60 minutes, as well as the peak and average global RapidRoute count per hour for the last 72 hours.
protocol <*protocol*>	Optional. Displays RapidRoute entries that use a specified protocol. Protocols can be specified by selecting one of the following: **ah** Displays Authentication Header (AH) Protocol RapidRoute entries. **esp** Displays Encapsulating Security Payload (ESP) Protocol RapidRoute entries. **fragment** Displays fragmented (FRAG) RapidRoute entries. **gre** Displays Generic Route Encapsulation (GRE) Protocol RapidRoute entries. **icmp6** Displays ICMPv6 RapidRoute entries. **tcp** Displays TCP RapidRoute entries. **udp** Displays UDP RapidRoute entries. **0** to **255** Displays other protocol types.
source <*ipv6 address*>	Optional. Displays RapidRoute entries for a specified source IPv6 address. IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).
source-port <*port*>	Optional. Displays RapidRoute entries for a specified TCP or UDP source port. Ports range from **0** to **65535**.
system-control-evc	Optional. Displays RapidRoute entries for the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Displays RapidRoute entries for the system management EVC.

type <*type*>	Optional. Displays RapidRoute entries of a specific type. Specified types include one of the following: **ineligible** Displays only ineligible RapidRoute entries. **rejected** Displays only rejected RapidRoute entries. **valid** Displays only valid RapidRoute entries.
wildcard	Optional. Displays wildcards for each IP interface.
interface <*interface*>	Optional. Limits the wildcard output to the specified interface. Interfaces are specified in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *group id]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an EFM group interface, use **efm-group 1**. Type **show ipv6 ffe wildcard interface ?** to display a complete list of valid interfaces.

Default Values

No default values are necessary for this command.

Command History

Release R10.4.0	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R11.3.0	Command was expanded to include the Ethernet in the first mile (EFM) group interface.
Release R11.4.0	Command was expanded to include the **fragment** option in the **protocol** parameter.
Release R11.10.0	Command was expanded to include the **peak** and **wildcard** parameters.
Release R13.7.0	Command was expanded to include the Gigabit Ethernet and virtual local area network (VLAN) interfaces.

Functional Notes

The **show ipv6 ffe** command can be further filtered by adding any combination of the following parameters:

destination <*ipv6 address*>
destination-port <*port*>
details
egress <*interface*>
egress ipsec <*rapidroute interface ID*>
icmp-type <*type*>
ingress <*interface*>

ingress ipsec <*rapidroute interface ID*>
protocol <*protocol*>
source <*ipv6 address*>
source-port <*port*>
type <*type*>

For example, the **destination** <*ipv6 address*> and **source** <*ipv6 address*> parameters can be used in conjunction with one another. In this case, the command would look like this:

#show ipv6 ffe destination 2001:DB8:1::1 source 2001:DB8:1::2

These parameters can be combined in any order, and as many times as is necessary to get the desired output.

*The **detail** keyword must be the last keyword in the command. For example, **show ipv6 ffe destination** <ipv6 address> **egress** <interface> **source-port** <port> **details** is acceptable, but **show ipv6 ffe destination** <ipv6 address> **details egress** <interface> is not.*

Data for the **peak history** parameters is presented as a percentage of the value configured with the command *ipv6 ffe max-entries <value> on page 1520*. Changing the **ipv6 ffe max-entries** value clears the related FFE peak information.

Usage Examples

The following is sample output from the **show ipv6 ffe** command:

```
>enable
#show ipv6 ffe
Timeout     TCP     UDP     ICMP    AH      ESP     GRE     Other
Age:        30m0s   30m0s   30m0s   30m0s   30m0s   30m0s   30m0s
Inactive:   15s     15s     15s     15s     15s     15s     15s
Type:  * valid, ! ineligible, - rejected
Flags: F firewall, N NAT, T altered ToS, D don't fragment, I IPsec
--------------------------------
Ingress: eth 0/1
   149 hits, 62553 misses, 0 drops

T   Proto Source          Destination     Specific    Age   Used  Drops  Flags
!   udp   2001:db8:1::1   2001:db8:1::9    3959       137   17s   10     0
!   udp   2001:db8:1::2   2001:db8:1::8    138        138   16s   0      0
!   udp   2001:db8:1::3   2001:db8:1::7    138        138   16s   0      0
!   udp   2001:db8:1::4   2001:db8:1::6     138       138   4s    0      0
!   udp   2001:db8:1::5   2001:db8:1::5     137       137   7s    2      0
!   tcp    2001:db8:1::6  2001:db8:1::4    2668       23    6s    36     0
Number of entries: 6 of 6 (4096 maximum)
--------------------------------
Total number of entries: 6 of 6 (16384 maximum)
```


The following is sample output from the **show ipv6 ffe details** command:

```
Timeout     TCP       UDP       ICMP      AH        ESP       GRE       Other
Age:        30m0s     30m0s     30m0s     30m0s     30m0s     30m0s     30m0s
Inactive:   15s       15s       15s       15s       15s       15s       15s
Type:  * valid, ! ineligible, - rejected
Flags: F firewall, N NAT, T altered ToS, D don't fragment, I IPsec
--------------------------------
Ingress: eth 0/1
   706189 hits, 45 misses, 0 drops
T Proto Source         Destination      Specific       Age   Used Drops Flags
* icmp  2001:db8:1::1 2001:db8:1::2 echo     13     13s    129     0     I
   egress: Outbound ESP SA 2
Number of entries: 1 of 1  (4096 maximum)
--------------------------------
Ingress: Inbound ESP SA 1
   129 hits, 1 misses, 0 drops
T Proto Source         Destination      Specific       Age   Used Drops Flags
* icmp  2001:db8:1::1 2001:db8:1::2 reply    13     13s    129     0     I
   egress: eth 0/1 (2001:db8:1::2)
Number of entries: 1 of 1  (4096 maximum)

--------------------------------
Ingress: Outbound ESP SA 2
   129 hits, 1 misses, 0 drops
T Proto Source         Destination      Specific         Age   Used    Drops    Flags
* esp   2001:db8:1::1 2001:db8:1::2  0x923dbab4   13s    129      0        I
   egress: hdlc 1
Number of entries: 1 of 1  (256 maximum)
--------------------------------
Total number of entries: 3 of 3  (16384 maximum)
```

The following is sample output from the **show ipv6 ffe** command when wildcards are in use; any field that has been wildcarded appears as **any**:

```
Timeout     TCP       UDP       ICMP      AH        ESP       GRE       Other
Age:        30m0s     30m0s     30m0s     30m0s     30m0s     30m0s     30m0s
Inactive:   15s       15s       15s       15s       15s       15s       15s

Exceptions: 0/217/0 (current/max/drops)

Type:  * valid, ! ineligible, - rejected
Flags: F firewall, N NAT, T altered ToS, D don't fragment, I IPsec, H hardware assist, i ingress filter,
     e egress filter
--------------------------------
Ingress: system-management-evc
   0 hits, 73 misses, 0 drops
```



```
T   Proto   ToS     Age     Used    Drops   Flags   Source    Destination
!   icmp6   any     8s        4     0               any       2001:db8:1::1, echo-request id: 269
!   icmp6   any     30s       1     0               any       2001:db8:1::2, type: 134 id:0
!   icmp6   any     5s       48     0               any       2001:db8:1::3, echo-request id: 269
Number of entries: 3 of 3 (4096 maximum)
```

The following is sample output from the **show ipv6 ffe wildcard interface eth 0/1** command:

```
>enable
#show ipv6 ffe wildcard eth 0/1
Field                                Wildcarded
============================         ============================
eth 0/1
    Source IP Address                :No
    Dest IP Address                  :No (always)
    IP Precedence                    :No
    IP DSCP                          :Yes
    IP Protocol (L4)                 :Yes
    TCP Source Port                  :Yes
    TCP Destination Port             :Yes
    UDP Source Port                  :Yes
    UDP Destination Port             :Yes
    ICMP Type, Code and ID           :Yes
    ESP SPI                          :Yes
    GRE Tunnel Key                   :Yes
```

show ipv6 ffe summary

Use the **show ipv6 ffe summary** command to display a summary of all the current Internet Protocol version 6 (IPv6) RapidRoute fast forwarding engine (FFE) entries.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following is sample output from the **show ipv6 ffe summary** command:

```
>enable
#show ipv6 ffe summary
Ingress          MaxEntries   Entries   Hits   Misses     Drops
---------        ----------   -------   ----   --------   -------
eth 0/1          4096         1         1000   200        11
eth 0/2.1        4096         1         1123   211        0
eth 0/2.2        4096         1         1467   301        0
                 ----------   -------   ----   --------   -------
          Global 16384        3         3590   712        11
```


show ipv6 interfaces

Use the **show ipv6 interfaces** command to display the status information for all Internet Protocol version 6 (IPv6) interfaces (or a specific IPv6 interface). This information includes IPv6 addressing, configured parameters, and any IPv6 capabilities in use. Variations of this command include:

show ipv6 interfaces
show ipv6 interfaces brief
show ipv6 interfaces <*ipv6 interface*>
show ipv6 interfaces <*ipv6 interface*> **prefix**
show ipv6 interfaces mef-ethernet <*slot/port*>
show ipv6 interfaces mef-ethernet <*slot/port*> **prefix**
show ipv6 interfaces system-control-evc
show ipv6 interfaces system-control-evc prefix
show ipv6 interfaces system-management-evc
show ipv6 interfaces system-management-evc prefix

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

brief	Optional. Displays an abbreviated version of interface statistics for all IPv6 interfaces.
<*ipv6 interface*>	Optional. Displays status information for a specific IPv6 interface. Specify an IPv6 interface in the format <*interface*> <*slot/port* | *interface id*>. For example, Point-to-Point Protocol (PPP) interface, enter **ppp 1**. If no interface is specified, status information for all IPv6 interfaces is displayed.
mef-ethernet <*slot/port*>	Optional. Displays status information for the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Displays status information for the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Displays status information for the system management EVC.
prefix	Optional. Displays the list of prefixes for the specified IPv6 interface.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Usage Examples

The following is sample output of the **show ipv6 interfaces** command, and displays information in brief format for the ethernet 0/1 interface:

```
>enable
#show ipv6 interfaces brief ethernet 0/1
eth 0/1 [UP/UP]
    FE80::2AO:C8FF:FE61:3082
    2003::2AO:C8FF:FE61:3082
```

show ipv6 mld groups link-local

Use the **show ipv6 mld groups link-local** command to display the known Multicast Listener Discovery (MLD) groups used by Internet Protocol version 6 (IPv6) features on the AOS router. Variations of this command include:

show ipv6 mld groups link-local
show ipv6 mld groups link-local <*interface*>
show ipv6 mld groups link-local vrf <*name*>
show ipv6 mld groups link-local vrf <*name*> <*interface*>

Syntax Description

<*interface*>	Optional. Specifies that only MLD groups registered on the specified interface are displayed. Specify an IPv6 interface in the format <*interface*> <*slot/port* | *interface id*>, for example, to use a Point-to-Point Protocol (PPP) interface, enter **ppp 1**.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance for which to display the MLD groups. If a VRF is not specified, MLD groups for the default (unnamed) VRF are displayed.

Default Values

No default values are necessary for this command.

Command History

Release R11.4.0	Command was introduced.

Usage Examples

The following example displays the MLD groups used on the Gigabit Ethernet subinterface **0/2.1**:

```
>enable
#show ipv6 mld groups link-local giga-eth 0/2.1
    MLD Connected Group Membership
    Group Address                 Interface          Uptime      Expires
    FF02::1                       giga-eth 0/2.1     13h32m32s   Never
    FF02::2                       giga-eth 0/2.1     13h32m32s   Never
    FF02::1:FF00:1234             giga-eth 0/2.1     13h32m32s   Never
    FF02::1:FF01:2CC              giga-eth 0/2.1     13h32m32s   Never
```

show ipv6 mld traffic

Use the **show ipv6 mld traffic** command to display the Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) traffic counters. Variations of this command include:

show ipv6 mld traffic
show ipv6 mld traffic vrf <*name*>

Syntax Description

vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance for which to clear the MLD traffic counters. If a VRF is not specified, MLD counters for the default (unnamed) VRF are displayed.

Default Values

No default values are necessary for this command.

Command History

Release R11.4.0	Command was introduced.

Usage Examples

The following example displays all MLD traffic counters:

```
>enable
#show ipv6 mld traffic
    MLD Traffic Counters
    Elapsed time since counters cleared: Never cleared

                                Sent            Received
    Valid MLD Packets           3263            1628
    Queries                     0               1628
    Reports                     3263            0
    Leaves                      0               0

    Errors:
    Malformed Packets                           0
    Non link-local source                       0
    Hop limit not equal to 1                    0
```

show ipv6 named-prefix

Use the **show ipv6 named-prefix** command to display information about the Internet Protocol version 6 (IPv6) named prefixes configured on the router. Information displayed includes which prefixes are assigned, how they are configured and delegated, and which interfaces are configured to be addressed using the named prefix.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example displays IPv6 named prefix information:

```
>enable
#show ipv6 named-prefix
!
IPv6 Prefix manualprefix, acquired via Manual configuration
    2001::/64 Valid lifetime infinite, preferred lifetime infinite
        Ethernet 0/2 (Address command)

IPv6 Prefix delegatedprefix, acquired via DHCP PD
    2001:1::/64 Valid lifetime 3202, preferred lifetime 1402
        Ethernet 0/3 (Address command)

IPv6 Prefix delegatedprefix, acquired via DHCP PD (DEPRECATED BY SERVER)
    2001:1::/64 Valid lifetime 132, preferred lifetime 0
        Ethernet 0/3 (Address command)
```


show ipv6 neighbors

Use the **show ipv6 neighbors** command to display the Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) cache. This cache contains information about IPv6 nodes that have been added to the cache, including the link-layer IPv6 address and the reachability state of that neighbor. Neighbor cache entries are created when there is a packet to send to an on-link destination, or when a neighbor solicitation (NS), router solicitation (RS), or router advertisement (RA) message is received. Variations of this command include:

show ipv6 neighbors
show ipv6 neighbors <*interface*>
show ipv6 neighbors <*interface*> <*ipv6 address*>
show ipv6 neighbors <*interface*> **statistics**
show ipv6 neighbors [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc]**
show ipv6 neighbors [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc]** <*ipv6 address*>
show ipv6 neighbors [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc] statistics**
show ipv6 neighbors statistics
show ipv6 neighbors vrf <*name*>
show ipv6 neighbors vrf <*name*> <*ipv6 address*>
show ipv6 neighbors vrf <*name*> **statistics**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*interface*>	Optional. Displays the neighbor cache information for a specified interface. IPv6 interfaces are specified in the <*interface*> <*slot/port* | *interface id*> format. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. If no interface is specified, information for all interfaces is displayed.
mef-ethernet <*slot/port*>	Optional. Displays the neighbor cache information for the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Displays the neighbor cache information for the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Displays the neighbor cache information for the system management EVC.

<ipv6 address>	Optional. Displays the neighbor cache information for a specified IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
statistics	Optional. Displays neighbor cache statistics and protocol interaction information for the neighbor cache.
vrf *<name>*	Optional. Displays the neighbor cache information for a specified virtual routing and forwarding (VRF) instance. If no VRF is specified, information for the unnamed default VRF is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output of the **show ipv6 neighbors** command, which displays all information for the ND cache:

```
>enable
#show ipv6 neighbors
IPv6 Address                    Age  Link-layer Addr  State   Interface
2002::1                          0   000f.352.3.2aba  REACH   eth 0/0
2003::ED9A:D1A3:BB9B:BDFF        0   0013.ce61.65b9   REACH   eth 0/1
20FF:11::ED9A:D1A3:BB9B:BDFF    18   0013.ce.61.65b9  STALE   eth 0/1
FE80::213:CEFF:FE61:65B9        10   0013.ce.61.65b9  DELAY   eth 0/1
FE80::20F:35FF:FE2E:2ABA         1   000f.352e.2aba   DELAY   eth 0/1
```


show ipv6 policy-sessions

Use the **show ipv6 policy-sessions** command to display a list of current Internet Protocol version 6 (IPv6) access control policy (ACP) associations in the IPv6 firewall. Current associations are active or recently active sessions allowed through the firewall. Refer to *ipv6 policy-class <ipv6 acp name> on page 1549* for information on configuring IPv6 ACPs. Variations of this command include:

show ipv6 policy-sessions
show ipv6 policy-sessions *<ipv6 acp name>*
show ipv6 policy-sessions any-vrf
show ipv6 policy-sessions vrf *<name>*
show ipv6 policy-sessions pending
show ipv6 policy-sessions pending *<ipv6 acp name>*
show ipv6 policy-sessions pending any-vrf
show ipv6 policy-sessions pending vrf *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv6 acp name>	Optional. Displays IPv6 policy class associations for the specified IPv6 ACP.
pending	Optional. Displays any currently pending policy sessions.
any-vrf	Optional. Displays information for all virtual routing and forwardings (VRFs) policy sessions.
vrf *<name>*	Optional. Specifies the particular firewall instance for which active policy sessions will be displayed. If no VRF is specified, policy sessions are displayed for the default VRF only.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the **pending** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **show ipv6 policy-sessions** command and displays information for IPv6 ACPs:

```
>enable
#show ipv6 policy-sessions
NOTE: The “Layer 4” info below for TCP and UDP is source port and dest port. For ICMPv6, it is ID and
    type/code. For all other protocols, it is unused.

Src VRF (if not default), Src policy-class:
Protocol (TTL) -> Dest VRF, Dest policy-class
    Src IPv6 Address                Layer 4
    Dest IPv6 Address               Layer 4
    ------------------------        ----------

Ipv6 policy-class PRIVATEV6:
icmpv6 (59) -> self
    2001:DB8:1:1::2                 0
    2001:DB8:1:1::1                 128/0
```


show ipv6 policy-stats

Use the **show ipv6 policy-stats** command to display a list of current Internet Protocol version 6 (IPv6) access control policy (ACP) statistics. Refer to *ipv6 policy-class <ipv6 acp name> on page 1549* for information on configuring IPv6 ACPs. Variations of this command include:

show ipv6 policy-stats
show ipv6 policy-stats *<ipv6 acp name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<ipv6 acp name>	Optional. Displays policy class statistics for a specific IPv6 ACP.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example displays a list of current IPv6 ACP statistics:

```
>enable
#show ipv6 policy-stats
```


show ipv6 prefix-list

Use the **show ipv6 prefix-list** command to display Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) prefix list information. Variations of this command include:

show ipv6 prefix-list *<name>*
show ipv6 prefix-list detail *<name>*
show ipv6 prefix-list summary *<name>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<name>	Shows information for a specific prefix list.
detail	Optional. Shows a listing of the specified prefix list rules and their hit counts.
summary	Optional. Shows summarized information about the specified prefix list.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

If the **show ipv6 prefix-list** command is issued with no arguments, a listing of the prefix-list rules, but no hit count statistics, is displayed.

Usage Examples

The following example displays information about the prefix list **TEST1**.

```
>enable
#show ipv6 prefix-list TEST1
ipv6 prefix-list TEST1: 4 entries
  seq 5 permit 0.0.0.0/0 ge 8 le 8
  seq 10 deny 0.0.0.0/0 ge 9 le 9
  seq 15 permit 0.0.0.0/0 ge 10 le 10
  seq 20 deny 0.0.0.0/0 ge 11
```


show ipv6 route

Use the **show ipv6 route** command to display the contents of the Internet Protocol version 6 (IPv6) route table. This table contains information about IPv6 networks and how to reach them. Variations of this command include:

show ipv6 route
show ipv6 route *<ipv6 address>*
show ipv6 route *<ipv6 address>* **longer-prefixes**
show ipv6 route *<ipv6 prefix/prefix-length>*
show ipv6 route *<ipv6 prefix/prefix-length>* **longer-prefixes**
show ipv6 route bgp
show ipv6 route bgp verbose
show ipv6 route connected
show ipv6 route ospf
show ipv6 route ospf verbose
show ipv6 route static
show ipv6 route static verbose
show ipv6 route summary
show ipv6 route summary realtime
show ipv6 route vrf *<name>*
show ipv6 route vrf *<name> <ipv6 address>*
show ipv6 route vrf *<name> <ipv6 address>* **longer-prefixes**
show ipv6 route vrf *<name> <ipv6 prefix/prefix-length>*
show ipv6 route vrf *<name> <ipv6 prefix/prefix-length>* **longer-prefixes**
show ipv6 route vrf *<name>* **bgp**
show ipv6 route vrf *<name>* **connected**
show ipv6 route vrf *<name>*
show ipv6 route vrf *<name>* **verbose**
show ipv6 route vrf *<name>* **static**
show ipv6 route vrf *<name>* **summary**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<ipv6 address>	Optional. Specifies a valid IPv6 address. IPv6 addresses should be expressed in colon hexadecimal notation (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<ipv6 prefix/prefix-length>	Optional. Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
bgp	Optional. Displays IPv6 route information for Border Gateway Protocol (BGP) configurations.
connected	Optional. Displays only the IPv6 routes for directly connected networks.
longer-prefixes	Optional. Displays only the IPv6 routes matching the specified network.
ospf	Optional. Displays only the Open Shortest Path First version 3 (OSPFv3) IPv6 routes.
static	Optional. Displays only the IPv6 routes that were statically entered.
summary	Optional. Displays a summary of all IPv6 route information.
summary realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.
verbose	Optional. Enables detailed messaging.
vrf *<name>*	Optional. Displays only the IPv6 routes for the specified virtual routing and forwarding (VRF).

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the **bgp** parameter.
Release R10.5.0	Command was expanded to include the **ospf** parameter.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example shows how to display IPv6 routes table information for the IPv6 address prefix **2001::/64**:

```
>enable
#show ipv6 route 2001::/64
Routing entry for 2001::/64
        Known via “static”
        Distance 1, metric 0
        Routing Next Hop(s):
            2002::1, via eth 0/1
             Route metric is 0
```

The following example shows output for the **show ipv6 route summary** command.

```
>enable
#show ipv6 route summary
Route Source            FIB         Local-RIB
    Connected            3           3
    Other               18          18

    Total               21          21
```

show ipv6 route named-prefix

Use the **show ipv6 route named-prefix** command to display all Internet Protocol version 6 (IPv6) routes generated by a named prefix.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example displays all IPv6 routes generated by a named prefix:

```
>enable
#show ipv6 route named-prefix
Codes: C-connected, S-static, O-OSPF, B-BGP
       E1-OSPF external type 1, E2-OSPF external type 2
       I-OSPF inter area, NP-named prefix, D-DHCPv6 PD

Gateway of last resort is not set

C   1::/64
    is directly connected, eth 0/1

NP      1::1:0:0:0/80
(1/0/0) via 1::1, Loopback
```


show ipv6 routers

Use the **show ipv6 routers** command to display information learned from router advertisement (RA) messages received from locally reachable routers when using Internet Protocol version 6 (IPv6). Variations of this command include:

show ipv6 routers
show ipv6 routers conflict
show ipv6 routers <*interface*>
show ipv6 routers <*interface*> **conflict**
show ipv6 routers [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc]**
show ipv6 routers [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc] conflict**
show ipv6 routers vrf <*name*>
show ipv6 routers vrf <*name*> **conflict**

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

conflict	Optional. Specifies that only information about routers whose advertisements are in conflict with current configurations are displayed.
<*interface*>	Optional. Displays information for the specified interface. Specify interfaces in the <*interface*> <*slot/port* | *interface id*> format. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**.
mef-ethernet <*slot/port*>	Optional. Displays information for the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Displays information for the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Displays information for the system management EVC.
vrf <*name*>	Optional. Displays only the IPv6 routes for the specified virtual routing and forwarding (VRF) instance. If no VRF is specified, information for the default VRF is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

In the following example, RA statistics for all interfaces on the default VRF are displayed:

```
>enable
#show ipv6 routers
Router FE80::20F:35FF:FE2E:2ABA on Ethernet 0/0, last update 1 min, CONFLICT
    Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
    Preference=Medium
    Reachable time 0 (unspecified) ms, Retransmit time 0 (unspecified) ms
    Prefix 2002::/64 on-link autoconfig
        Valid lifetime 8002, preferred lifetime 2008
```


show ipv6 traffic

Use the **show ipv6 traffic** command to display system-wide Internet Protocol version 6 (IPv6) and Internet Control Message Protocol version 6 (ICMPv6) traffic statistics. Variations of this command include:

show ipv6 traffic
show ipv6 traffic realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example displays all IPv6 traffic statistics:

>**enable**
#show ipv6 traffic
IPv6 statistics:
Rcvd: 0 total, 9 local destination
0 header errors, 0 address errors
0 unknown protocol, 0 discards
0 truncated, 0 bad hop counts
Sent: 0 locally generated, 59 forwarded
0 no route, 0 discards
Frag: 0 reassemble required, 0 reassembled, 0 couldn’t reassemble
0 created, 0 fragmented, 0 couldn’t fragment

show isdn-group <*number*>

Use the **show isdn-group** command to display integrated services digital network (ISDN) group information.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<number>	Displays information for a specific ISDN group. Valid range is **1** to **255**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays information for ISDN group **5**:

```
>enable
#show isdn-group 5
```


show isdn-number-template

Use the **show isdn-number-template** command to display integrated services digital network (ISDN) number templates. Variations of this command include:

show isdn-number-template
show isdn-number-template *<value>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<value>	Optional. Displays information about a specific number template. Valid range is **1** to **255**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays information for ISDN number template **0**:

```
>enable
#show isdn-number-template 0
Type          ID      Prefix    Pattern
Subscriber    0                 911
#
```


show isdn resource

Use the **show isdn resource** command to display integrated services digital network (ISDN) resource information. Variations of this command include:

show isdn resource
show isdn resource realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example displays ISDN resource information:

>enable
#show isdn resource

Interface: ChannelId	Channel State:GID	Trunk: Appearance	Appearance State	Slot/Prt: B-Channel	Call State
pri 1:0	Reserved:1	T01:2	TAS_Connect	1/1:21	OutgoingConnect
pri 1:1	Reserved:1	T01:0	TAS_Alerting	1/1:23	IncomingAlertingSent
pri 1:2	Available	---	---	---	---
pri 1:3	Available	---	---	---	---
pri 1:4	Available	---	---	---	---
pri 1:5	Available	---	---	---	---
pri 1:6	Available	---	---	---	---
pri 1:7	Available	---	---	---	---
pri 1:8	Available	---	---	---	---
pri 1:9	Available	---	---	---	---
pri 1:10	Available	---	---	---	---
pri 1:11	Available	---	---	---	---
pri 1:12	Available	---	---	---	---
pri 1:13	Available	---	---	---	---
pri 1:14	Available	---	---	---	---
pri 1:15	Available	---	---	---	---
pri 1:16	Available	---	---	---	---
pri 1:17	Available	---	---	---	---
pri 1:18	Available	---	---	---	---
pri 1:19	Available	---	---	---	---
pri 1:20	Available	---	---	---	---
pri 1:21	Available	---	---	---	---
pri 1:22	Available	---	---	---	---

show license

Use the **show license** command to display AOS feature license information including: errors, features, keys, request keys, status and usage. Variations of this command include:

show license [verbose]
show license errors
show license features
show license keys
show license request key
show license status current [verbose]
show license status deprecated [verbose]
show license status inactive [verbose]
show license status installed [verbose]
show license status obsolete [verbose]
show license status partial
show license status reboot [verbose]
show license status remove [verbose]
show license status running [verbose]
show license time
show license usage

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

errors	Optional. Displays the license errors detected during startup.
features	Optional. Displays all licensable features available on the unit.
keys	Optional. Displays archived license keys.
request key	Optional. Displays the current license request key.
status	Displays the license status information.
current	Displays the status of current licenses.
deprecated	Displays the status of deprecated licenses.
inactive	Displays the status of inactive licenses.
installed	Displays the status of installed licenses.
obsolete	Displays the status of obsolete licenses.
partial	Displays information for licenses that have a mixture of statuses.
reboot	Displays the status of licenses that will activate upon reboot.

remove	Displays the status of licenses that will be removed upon reboot.
running	Displays the status of currently active licenses.
time	Optional. Displays time-based information about the license (such as expiration).
usage	Optional. Displays license usage information.
verbose	Optional. Displays detailed license information.

Default Values

No default values are necessary for this command.

Command History

Release R11.8.0	Command was introduced.
Release R12.1.0	Command was expanded to include the **time** parameter. In addition, command output was modified for virtual AOS (vAOS) instances.

Functional Notes

AOS uses two types of keys for enabling additional licensed AOS features. The license key is requested from the Adtran licensing portal and installed on the AOS device in order to activate additional features. This process of requesting a license key requires a second key, called a license request key (or a challenge key). The license request key is a unique key generated by AOS and contains information about the unit that validates it for a one time use only. Once a license key has been installed, the license request key is cleared and no longer valid.

The **license request key** command will not display a key until the **license request key generate** command has been issued for the first time. Generating a new license request key clears any previous license request keys, whether or not they were used through the Adtran licensing portal.

Usage Examples

The following is sample output from the **show license keys** command:

>**enable**
#show license keys

********License Status: Current********

-----BEGIN LICENSE KEY-----
License Serial Num: 12345678
License Part Num: 1962SBCF50
Device Serial Num: LBADTN0000000
-----BEGIN BODY-----
RGV2aWNlU2VyaWFsTnVtPUxCQURUTjAwMDAwMDANCkxpY2Vuc2VWZXJzaW9uPWRvY3VtZW50YXRpb25fZGVtbw0KRW52ZWxvcGU9V2UgaG9sZCB0aGVzZSB0cnV0aHMgdG8gYmUgc2VsZi1ldmlkZW50LCB0aGF0IGFsbCBtZW4gYXJlIGNyZWF0ZWQgZXF1YWwsIHRoYXQgdGhleSBhcmUgZW5kb3dlZCBieSB0aGVpciBDcmVhdG9yIHdpdGggY2VydGFpbiB1bmFsaWVuYWJsZSBSaWdodHMsIHRoYXQgYW

1vbmcgdGhlc2UgYXJlIExpZmUsIExpYmVydHkgYW5kIHRoZSBwdXJzdWl0IG9mIEhhcHBpbmVzcy4=
-----END BODY-----
-----BEGIN AUTHENTICATION-----
Rm91ciBzY29yZSBhbmQgc2V2ZW4geWVhcnMgYWdvIG91ciBmYXRoZXJzIGJyb3VnaHQgZm9ydGgg
b24gdGhpcyBjb250aW5lbnQsIGEgbmV3IG5hdGlvbiwgY29uY2VpdmVkIGluIExpYmVydHksIGFu
ZCBkZWRpY2F0ZWQgdG8gdGhlIHByb3Bvc2l0aW9uIHRoYXQgYWxsIG1lbiBhcmUgZCBl
cXVhbC4=
-----END AUTHENTICATION-----
-----END LICENSE KEY-----

show lldp

Use the **show lldp** command to display the Link Layer Discovery Protocol (LLDP) transmit interval and transmitted time to live (TTL).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

The TTL is calculated by multiplying the transmit interval by the TTL multiplier. For more information, refer to the command *lldp on page 1573*.

Usage Examples

The following is sample output for the LLDP timer configuration:

```
>enable
#show lldp
Global LLDP information:
Sending LLDP packets every 30 seconds
Sending TTL of 120 seconds
```


show lldp device <*name*>

Use the **show lldp device** command to display neighbor information about an adjacent device on the same IEEE 802 local area network (LAN).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Specifies the system name of the neighbor to display.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

If there is more than one neighbor with the same system name, all neighbors with that system name will be displayed.

Usage Examples

The following example shows specific information about a neighbor for the system name **Router**:

```
>enable
#show lldp device Router
Chassis ID: 00:A0:C8:02:DD:2A (MAC Address)
    System Name: Router
    Device Port: eth 0/1 (Locally Assigned)
    Holdtime: 30
    Platform: NetVanta 3305
    Software: Version: 08.00.22.sw1.D, Date: Mon Nov 01 10:28:55 2004
    Capabilities: Bridge, Router
    Enabled Capabilities: Router
    Local Port: eth 0/3
    Management Addresses:
    Address Type: IP version 4, Address: 10.23.10.10
```


show lldp interface

Use the **show lldp interface** command to display Link Layer Discovery Protocol (LLDP) configuration and statistics for interfaces on this device. Variations of this command include:

show lldp interface
show lldp interface *<interface>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Optional. Displays the information for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show lldp interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet and gigabit switchport interfaces.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example shows LLDP statistics for the Ethernet 0/1 interface:

>**enable**
#show lldp interface ethernet 0/1
eth 0/1 (TX/RX)
    0 packets input
    0 input errors
    0 TLV errors, 0 TLVs Discarded
    0 packets discarded
    8799 packets output
    0 neighbor ageouts

show lldp neighbors

Use the **show lldp neighbors** command to display information about neighbors of this device learned about via Link Layer Discovery Protocol (LLDP). Variations of this command include:

show lldp neighbors
show lldp neighbors detail
show lldp neighbors <*interface*>
show lldp neighbors interface <*interface*> **detail**
show lldp neighbors med
show lldp neighbors realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

detail	Optional. Shows detailed neighbor information for all LLDP neighbors or neighbors connected to the specified interface or interface type.
interface <*interface*>	Optional. Displays a summary of all neighbors learned about through the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show lldp neighbors interface ?** for a complete list of applicable interfaces.
med	Optional. Displays neighbors that are capable of supporting LLDP-Media Endpoint Discovery (LLDP-MED).
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.2	Command was expanded to include the **med** parameter.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet and gigabit switchport interfaces.
Release R11.5.0	Command was expanded to include inventory information if transmitted by the endpoint when using the **detail** parameter.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example shows detailed information about a device's neighbors:

```
>enable
#show lldp neighbors interface eth 0/3 detail
Chassis ID: 00:A0:C8:02:DD:2A (MAC Address)
 System Name: Router
 Device Port: eth 0/1 (Locally Assigned)
 Holdtime: 38
 Platform: NetVanta 3305
 Software: Version: 08.00.22.sw1.D, Date: Mon Nov 01 10:28:55 2004
 Capabilities: Bridge, Router
 Enabled Capabilities: Router
 Local Port: eth 0/3
 Management Addresses:
   Address Type: IP version 4, Address: 10.23.10.10
Interface Type: Interface Index, Interface Id: 2
```


The following example shows LLDP-MED capable neighbors connected to a device:

```
>enable
#show lldp neighbors med
Capability Codes: R - Router, B - Bridge, H - Host, D - DOCSIS Device,
                  W - WLAN Access Point, r - Repeater, T - Telephone

System Name                      Port ID                  TTL       Cap.       Platform           Local Int
-------------------------------- ------------------------ --------- ---------- ------------------ ----------------
URL 5000@10.22.41                08:00:0F:2C:AB            96       --B--T--                      swx 0/2
```

show lldp neighbors statistics

Use the **show lldp neighbors statistics** command to display statistics about Link Layer Discovery Protocol (LLDP) neighbor table actions.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

This command shows information about the changes in this device's neighbor table. The information displayed indicates the last time a neighbor was added to or removed from the table, as well as the number of times neighbors were inserted into or deleted from the table.

System Last Change Time	Shows the time at which the most recent change occurred in the neighbor table.
Inserts	Shows the number of times neighbors have been added to the table.
Deletes	Shows how many times neighbors have been deleted from the table because an interface was shut down.
Drops	Shows how many times the insertion of a new neighbor into the table failed because the table was full.
Age Outs	Shows how many times neighbors have been removed from the table because no new updates were received from that neighbor before its time to live (TTL) timer expired.

Usage Examples

The following is sample output for this command:

>**enable**
#show lldp neighbors statistics

System Last Change Time	Inserts	Deletes	Drops	Age Outs
10-15-2004 14:24:56	55	3	1	1

show load-protect

Use the **show load-protect** command to display configuration parameters and current statistics for the load protect feature.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following is sample output from the **show load-protect** command:

#show load-protect

```
Mode: cli
Timeout: 300ms
Congestion method: percentage increase/decrease
increase percentage: 10%
decrease percentage: 90%

Protocol             Queue     Processed  CIR       CBS
==================== ========= ========= ========= ====
dhcp:                5         0          0         0
icmp:                2         0          0         0
icmp-unreachable:    6         0          0         0
ipv6-nd:             1         0          0         0
arp:                 1         8          0         0
radius:              6         0          0         0
ntp:                 6         0          0         0
snmp:                6         0          0         0
ssh:                 3         0          0         0
```


vrrp:	4	0	0	0
vrrpv3:	4	0	0	0
ipv6-hop-by-hop:	6	0	0	0
(default)	0	170	0	0

Queue	Weight	Processed	No Buffers
0(default)	1024	170	0
1	128	8	0
2	128	8	0
3	128	8	0
4	128	1231351	0
5	128	8	0
6	128	8	0
7	128	8	0

show logging forwarding

Use the **show logging forwarding** command to display current configuration settings for the logging forwarding feature. The AOS syslog event feature is enabled using the command *logging forwarding on on page 1600*.

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R12.3.0	Command was introduced.

Usage Examples

To display the current configuration of logging forwarding, enter the command as follows:

```
>enable
#show logging forwarding
```


show mac address-table

Use the **show mac address-table** command to display all static and dynamic entries in the medium access control (MAC) address table for all virtual local area networks (VLANs) and physical interfaces.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show mac address-table** command:

```
>enable
#show mac address-table
Mac Address Table
------------------------------------------
Vlan    Mac Address         Type        Ports
1       aa:bb:ee:d1:c2:33   STATIC      eth 0/18
1       00:00:00:00:00:00   STATIC      CPU
2       00:90:2b:7d:30:00   DYNAMIC     eth 0/1
2       00:a0:c8:00:8e:a6   DYNAMIC     eth 0/1
2       00:a0:c8:00:8f:ba   DYNAMIC     eth 0/1
2       00:a0:c8:00:8f:73   DYNAMIC     eth 0/1
2       00:a0:c8:00:00:00   DYNAMIC     eth 0/1
2       00:a0:c8:01:ff:02   DYNAMIC     eth 0/1
2       00:a0:c8:01:09:d3   DYNAMIC     eth 0/1
2       00:a0:c8:01:13:34   DYNAMIC     eth 0/1
2       00:a0:c8:01:14:4a   DYNAMIC     eth 0/1
2       00:a0:c8:03:95:4b   DYNAMIC     eth 0/1
2       00:a0:c8:05:00:89   DYNAMIC     eth 0/1
```


show mac address-table address

Use the **show mac address-table address** command to display all medium access control (MAC) addresses known by AOS. Variations of this command include the following:

show mac address-table address <*mac address*>
show mac address-table address <*mac address*> **interface** <*interface*>
show mac address-table address <*mac address*> **interface** <*interface*> **vlan** <*vlan id*>
show mac address-table address <*mac address*> **vlan** <*vlan id*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*mac address*>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
interface <*interface*>	Optional. Shows information for a specific interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show mac address-table address interface ?** for a list of valid interfaces.
vlan <*vlan id*>	Optional. Specifies a valid virtual local area network (VLAN) interface ID. Range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following is sample output from the **show mac address-table address** command displays information regarding a specific MAC address from the MAC address table:

```
>enable
#show mac address-table address 00:a0:c8:7d:30:00
Mac Address Table
------------------------------------------
Vlan    Mac Address          Type         Ports
--------  -------------------  ---------  -----------
2       00:a0:c8:7d:30:00    DYNAMIC    eth 0/1
```

The following is sample output from the **show mac address-table address** command displays information regarding a specific MAC address and interface from the MAC address table:

```
>enable
#show mac address-table address 00:a0:c8:7d:30:00 ethernet 0/1
Mac Address Table
------------------------------------------
Vlan    Mac Address          Type         Ports
--------  -------------------  ---------  -----------
2       00:a0:c8:7d:30:00    DYNAMIC    eth 0/1
Total Mac Addresses for this criterion: 1
#
```


show mac address-table aging-time

Use the **show mac address-table aging-time** command to display information regarding the amount of time dynamic entries remain in the medium access control (MAC) address table.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show mac address-table aging-time** command for a switch configured with an address-table aging-time:

```
>enable
#show mac address-table aging-time
Aging Time
----------
300 Seconds
```


show mac address-table count

Use the **show mac address-table count** command to display information regarding the number of medium access control (MAC) addresses in use (both static and dynamic).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show mac address-table count** command:

```
>enable
#show mac address-table count
Mac Table Entries:
--------------------------
Dynamic Address Count: 19
Static Address Count: 3
Total Mac Addresses: 23
Total Mac Address Space Available: 8169
```


show mac address-table dynamic

Use the **show mac address-table dynamic** command to display all dynamic medium access control (MAC) addresses learned by AOS. Variations of this command include the following:

show mac address-table dynamic
show mac address-table dynamic address *<mac address>*
show mac address-table dynamic address *<mac address>* **interface** *<interface>*
show mac address-table dynamic address *<mac address>* **interface** *<interface>* **vlan** *<vlan id>*
show mac address-table dynamic address *<mac address>* **vlan** *<vlan id>*
show mac address-table dynamic interface *<interface>*
show mac address-table dynamic interface *<interface>* **vlan** *<vlan id>*
show mac address-table dynamic vlan *<vlan id>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

address *<mac address>*	Optional. Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
interface *<interface>*	Optional. Shows information for a specific interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show mac address-table dynamic interface ?** for a list of valid interfaces.
vlan *<vlan id>*	Optional. Specifies a valid virtual local area network (VLAN) interface ID. Range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following is sample output from the **show mac address-table dynamic** command:

```
>enable
#show mac address-table dynamic
Mac Address Table
----------------------------
Vlan    Mac Address          Type        Ports
-------  -------------------  --------    --------
 1       00:a0:c8:7d:30:00    DYNAMIC     eth 0/1
 1       00:a0:c8:05:89:09    DYNAMIC     eth 0/2
 1       00:a0:c8:07:d9:d2    DYNAMIC     eth 0/5
 1       00:a0:c8:07:d9:19    DYNAMIC     eth 0/7
 1       00:a0:c8:09:95:6b    DYNAMIC     eth 0/7
 1       00:a0:c8:0a:2d:7c    DYNAMIC     eth 0/12
 1       00:a0:c8:f6:e9:a6    DYNAMIC     eth 0/24
 1       00:a0:c8:01:0a:ef    DYNAMIC     eth 0/23
 1       00:a0:c8:0c:74:80    DYNAMIC     eth 0/20
 1       00:a0:c8:15:5a:9f    DYNAMIC     eth 0/7
 1       00:a0:c8:6c:71:49    DYNAMIC     eth 0/2
 1       00:a0:c8:77:78:c1    DYNAMIC     eth 0/3
 1       00:a0:c8:6b:53:7b    DYNAMIC     eth 0/4
 1       00:a0:c8:72:e6:d6    DYNAMIC     giga-eth 0/2
 1       00:a0:c8:05:00:e6    DYNAMIC     giga-eth 0/1
Total Mac Addresses for this criterion: 15
```

show mac address-table interface

Use the **show mac address-table interface** command to display information regarding medium access control (MAC) address table entries specific to a certain interface. Variations of this command include:

show mac address-table interface <*interface*>
show mac address-table interface <*interface*> **vlan** <*vlan id*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*interface*>	*Shows information for a specific interface type.* Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. *Type* **show mac address-table interface ?** *for a list of valid interfaces.*
vlan <*vlan id*>	Optional. Shows address-table information related to a specific virtual local area network (VLAN). Valid range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following is sample output from the **show mac address-table interface eth 0/1** command displaying MAC address-table entries specifically on Ethernet 0/1:

>**enable**
#show mac address-table interface ethernet 0/1
Mac Address Table

Vlan	Mac Address	Type	Ports
2	00:90:2b:7d:30:00	DYNAMIC	eth 0/1
2	00:a0:c8:05:00:ac	DYNAMIC	eth 0/1
2	00:a0:c8:05:00:ad	DYNAMIC	eth 0/1
2	00:a0:c8:05:00:c2	DYNAMIC	eth 0/1
2	00:a0:c8:05:01:6e	DYNAMIC	eth 0/1
2	00:a0:c8:09:95:6b	DYNAMIC	eth 0/1
2	00:a0:c8:0a:2d:7c	DYNAMIC	eth 0/1

Total Mac Addresses for this criterion: 7

show mac address-table multicast

Use the **show mac address-table multicast** command to display all multicast medium access control (MAC) addresses known by AOS. Variations of this command include the following:

show mac address-table multicast
show mac address-table multicast count
show mac address-table multicast igmp-snooping
show mac address-table multicast igmp-snooping count
show mac address-table multicast user
show mac address-table multicast user count
show mac address-table multicast vlan <*vlan id*>
show mac address-table multicast vlan <*vlan id*> **count**
show mac address-table multicast vlan <*vlan id*> **igmp-snooping**
show mac address-table multicast vlan <*vlan id*> **igmp-snooping count**
show mac address-table multicast vlan <*vlan id*> **user**
show mac address-table multicast vlan <*vlan id*> **user count**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

count	Optional. Displays the multicast address count.
igmp-snooping	Optional. Displays MAC addresses learned via Internet Group Management Protocol (IGMP) snooping.
user	Optional. Displays static MAC addresses entered by the user.
vlan <*vlan id*>	Optional. Displays address table information related to a specific virtual local area network (VLAN). Valid range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show mac address-table multicast** command:

```
>enable
#show mac address-table multicast
Multicast Mac Address Table
-----------------------------------------
Vlan    Mac Address             Type        Ports
------  ------------------      --------    --------
1       01:00:5e:00:01:01         igmp      swx 0/10
1       01:00:5e:7f:ff:fa         igmp      swx 0/24
Total Mac Addresses for this criterion: 2
```

show mac address-table static

Use the **show mac address-table static** command to display all static medium access control (MAC) addresses known by AOS. Variations of this command include the following:

show mac address-table static
show mac address-table static address *<mac address>*
show mac address-table static address *<mac address>* **interface** *<interface>*
show mac address-table static address *<mac address>* **interface** *<interface>* **vlan** *<vlan id>*
show mac address-table static address *<mac address>* **vlan** *<vlan id>*
show mac address-table static interface *<interface>*
show mac address-table static interface *<interface>* **vlan** *<vlan id>*
show mac address-table static vlan *<vlan id>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

address *<mac address>*	Optional. Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
interface *<interface>*	Optional. Shows information for a specific interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show mac address-table static interface ?** for a list of valid interfaces.
vlan *<vlan id>*	Optional. Shows address-table information related to a specific virtual local area network (VLAN). Valid range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following is sample output from the **show mac address-table static** command:

```
>enable
#show mac address-table static
Mac Address Table
Vlan    Mac Address          Type       Ports
------  -------------------  --------   --------
 1      00:a0:c8:00:88:40    STATIC     CPU
Total Mac Addresses for this criterion: 1
```

show mac limits

Use the **show mac limits** command to display the configured maximum allowed media access control (MAC) addresses on the AOS device. The current number of MAC addresses and learned MAC addresses for each interface are displayed.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example displays the MAC addresses associated with each configured interface:

```
>enable
#show mac limits
```

Port	Max Allowed	Current	Learned
Gigabit-Ethernet 0/1	Disabled		
Gigabit-Ethernet 0/2	5	2	
Gigabit-Ethernet 0/3	10	1	
Gigabit-Ethernet 0/4	Disabled		
Gigabit-Ethernet 0/5	10	0	
Global Limit	1024	3	

show mail-client

Use the **show mail-client** command to display statistical summary information for mail agents. Variations of this command include:

show mail-client

show mail-client *<agent name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<agent name>	Optional. Specifies only statistics for the named mail agent are displayed.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example displays statistical information for mail agent **myagent**:

```
>enable
#show mail-client myagent
Mail-client myagent is ENABLED
    Capture output when track mail becomes PASS
    Send message when track T becomes PASS
    Send TO: joesmith@company.com

    6 output captures triggered
      18 commands captured
      6 command errors
         2 unrecognized commands
         4 truncated commands
    5 emails sent
    Last email sent on 2/29/2008 at 16:20:10 PM
```


show mail-client body <*agent name*>

Use the **show mail-client body** command to display the current buffer content for the body of the email message in queue for a specific mail agent.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*agent name*>	Specifies the mail agent buffer to display.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example displays the email body buffer content for **myagent** mail agent:

```
>enable
#show mail-client body myagent
```


show media-gateway

Use the **show media-gateway** command to show cumulative totals for all Realtime Transport Protocol (RTP) channels. Variations of this command include:

show media-gateway
show media-gateway channel
show media-gateway channel <*slot/dsp.channel*>
show media-gateway info
show media-gateway session
show media-gateway session <*slot/dsp.channel*>
show media-gateway summary
show media-gateway summary active

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*slot/dsp.channel*>	Optional. Specifies the ID of the media gateway channel to be displayed in the format *slot/dsp.channel*.
channel	Optional. Shows cumulative totals for individual RTP channels.
info	Optional. Shows media-gateway information.
session	Optional. Shows current RTP sessions.
summary	Optional. Shows summary of last active and current RTP sessions.
active	Optional. Shows summary of currently active RTP sessions.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows sample output from the **show media-gateway** command:

```
>enable
#show media-gateway

Media Gateway
  1 slots, 2 DSPs, 60 channels
  6 total sessions, 1 active sessions,
  00:00:11 total session duration
  Last clearing of counters: never
Receive
  601 total rx packets, 96160 total rx bytes
  Jitter Buffer Totals:
  0 out of order packets
  0 early arrival discards
  0 late arrival discards
  0 buffer full discards
  0 unknown packets
  13 flushed packets
Transmit
  647 total tx packets, 103520 total tx bytes
#
```

The following example shows sample output from the **show media-gateway info** command:

```
>enable
#show media-gateway info
slot 0, DSP 1
   DSP software version: G2.R10.5.0.0
   DSP hardware version: Freescale MSC7119
   DSP utilization: 49%
   maximum DSP utilization: 52%
   free packet buffers: 5998
   total channels: 30
   active channels: 0
   DSP uptime: 2d 23:42:10

slot 0, DSP 2
   DSP software version: G2.R10.5.0.0
   DSP hardware version: Freescale MSC7119
   DSP utilization: 49%
   maximum DSP utilization: 51%
   free packet buffers: 5998
   total channels: 30
   active channels: 0
   DSP uptime: 2d 23:42:04

    system uptime: 2d 23:42:18
```

show mef

Use the **show mef** command to display Metro Ethernet Forum (MEF) Ethernet component configuration and state information. Variations of this command include:

show mef
show mef connections
show mef connections discard
show mef connections evc <*name*>
show mef connections evc-map <*name*>
show mef connections men-port efm-group <*group id*>
show mef connections policer <*name*>
show mef connections uni mef-ethernet <*name*>
show mef evc-map
show mef evc-map <*name*>
show mef evc
show mef evc <*name*>
show mef policer
show mef policer <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

connections	Optional. Displays information on all MEF Ethernet connections.
discard	Optional. Displays discard connections.
evc <*name*>	Optional. Displays connection information on the specified Ethernet virtual connection (EVC).
evc-map <*name*>	Optional. Displays connection information on the specified EVC map.
men-port efm-group <*group id*>	Optional. Displays connection information for the specified Metro Ethernet network (MEN) Ethernet in the first mile (EFM) group.
policer <*name*>	Optional. Displays connection information on the specified EVC policer profile.
uni mef-ethernet <*name*>	Optional. Displays connection information on the specified user network Metro Ethernet interface.
evc-map	Optional. Displays the MEN priority and MEN queue information for all configured EVC maps.

evc-map <*name*>	Optional. Displays the MEN priority and MEN queue information for the specified EVC map.
evc	Optional. Displays status, s-tag, CE VLAN preservation, and connected EVC map information for all configured EVCs.
evc <*name*>	Optional. Displays status, s-tag, CE VLAN preservation, and connected EVC map information for the specified EVC.
policer	Optional. Displays configuration information for all EVC policer policies.
policer <*name*>	Optional. Displays configuration information for the specified EVC policer policy.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following is sample output from the **show mef** command:

```
#show mef
MEN Configured EVCs for efm-group 1 :
2213 3216

EVC DATA : Admin UP Protocol Connected UP

Connected to MEN Port efm-group 1
Connected to EVC Map DATA

Tag 3216
Preserve CE VLAN No

EVC DEFAULT : Admin UP Protocol Connected UP
Connected to MEN Port efm-group 1
Connected to EVC Map DEFAULT
Tag 2213
Preserve CE VLAN Yes

EVC Map DATA : Admin UP Protocol Connected UP
Connected to UNI mef-ethernet 1/1
Connected to EVC DATA
MEN Priority Inherit
MEN Queue Inherit
```

EVC Map DEFAULT : Admin UP Protocol Connected UP
Connected to UNI mef-ethernet 1/1
Connected to EVC DEFAULT
MEN Priority Inherit
MEN Queue Inherit

Connection : EVC Map DATA
UNI mef-ethernet 1/1
EVC DATA
MEN Port efm-group 1
Connection Status Connected UP

Connection : EVC Map DEFAULT
UNI mef-ethernet 1/1
EVC DEFAULT
MEN Port efm-group 1
Connection Status Connected UP#

show memory

Use the **show memory** command to display statistics regarding memory, including memory allocation and buffer use statistics. Shows how memory is in use (broken down by memory size) and how much memory is free. Variations of this command include:

show memory heap
show memory heap realtime
show memory uncached-heap

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

heap	Shows how much memory is in use (broken down by memory block size) and how much memory is free.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.
uncached-heap	Shows how much memory has been set aside to be used without memory caching, how much memory is being used, and how much memory is free.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show memory heap** command:

>**enable**
#show memory heap
Memory Heap:
  HeapFree: 2935792
  HeapSize: 8522736
Block Managers:

Mgr	Size	Used	Free	Max-Used
0	0	58	0	58
1	16	1263	10	1273
2	48	1225	2	1227
3	112	432	2	434
4	240	140	3	143
5	496	72	2	74
6	1008	76	1	26
7	2032	25	1	26
8	4080	2	1	3
9	8176	31	1	32
10	16368	8	0	8
11	32752	5	1	6
12	65520	3	0	30
13	131056	0	0	0

show mgcp-endpoint

Use the **show mgcp-endpoint** command to display configuration statistics for all configured Media Gateway Control Protocol (MGCP) endpoints. Variations of this command include:

show mgcp-endpoint
show mgcp-endpoint verbose

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

verbose	Optional. Enables detailed messaging.

Default Values

No default values are necessary for this command.

Command History

Release A2	Command was introduced.

Usage Examples

The following is sample output from the **show mgcp-endpoint** command:

```
#show mgcp-endpoint
        Endpoint: 1
        Name   : aaln/1
        FXS    : 0/1
        State  : Connected

        Endpoint: 2
        Name   : aaln/2
        FXS    : 0/2
        State  : Connected

        Endpoint: 3
        Name   : aaln/3
        FXS    : 0/3
        State  : Connected

        Endpoint: 4
        Name   : aaln/4
        FXS    : 0/4
        State  : Connected
```


show modules

Use the **show modules** command displays information on the current system setup. Variations of this command include:

show modules
show modules detailed

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detailed	Optional. Displays more detailed information in the output.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.1.0	Command was expanded to include the **detailed** parameter.
Release R12.1.0	Command output was modified for virtual AOS (vAOS) instances.

Usage Examples

The following example displays the modules installed in the unit.

```
>enable
#show modules
```

Slot	Port	Type	Part Number	Software Version
0	1	VPN Module	1202368L1	R10.11.0.E
1	1	T3 WAN	Not Available	Not Available
2	1	E1 VIM	Not Available	Not Available

show monitor session

Use the **show monitor session** command to display information regarding a specified monitor session or to display this information for all sessions. Variations of this command include:

show monitor session <*number*>
show monitor session all

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*number*>	Displays information for a single specific monitor session.
all	Displays all sessions.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show monitor session** command:

```
>enable
#show monitor session 1
Monitor Session 1
-----------------
Source Ports:
   RX Only:   None
   TX Only:   None
   Both:      eth 0/2, eth 0/3
Destination Port: eth 0/6
```


show name-server

Use the **show name-server** command to display the current domain naming system (DNS) name server's address and the source of its addresses. Address sources include Dynamic Host Control Protocol version 4 (DHCPv4), DHCP version 6 (DHCPv6), Point-to-Point Protocol and Internet Protocol Control Protocol (PPP-IPCP), and user configured addresses. Variations of this command include:

show name-server
show name-server realtime
show name-server vrf <*name*>
show name-server vrf <*name*> **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

realtime	Optional. Displays the name server information in real time.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance for which to display name server address information. If a VRF instance is not specified, name server information for the default VRF instance is displayed.

Default Values

No default values are necessary for this command.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example shows output from the **show name-server** command:

```
>enable
#show name-server
 Current          Name server address                  Source
 ------------------------------------------------------------------------------------------------
                  2000:ef0a::1500:37ag:362:ed          DHCPv6
   proxy -->      2000:a50:1a0e::1500:eddf             DHCPv6
                  10.23.115.254                        DHCPv4
   client -->     192.168.101.1                        PPP
                  8.8.8.8                              User
                  8.8.4.4                              User
```

show network-forensics ip dhcp

Use the **show network-forensics ip dhcp** command to display collected Dynamic Host Configuration Protocol (DHCP) information for clients connected to the network. The display of the collected information can be for all connected clients or for a specific client. Variations of this command include:

show network-forensics ip dhcp
show network-forensics ip dhcp hostname <*hostname*>
show network-forensics ip dhcp interface gigabit-switchport <*slot/port*>
show network-forensics ip dhcp ip <*ip address*>
show network-forensics ip dhcp mac <*mac address*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

hostname <*hostname*>	Optional. Displays DHCP information for the client with the specified host name.
interface gigabit-switchport <*slot/port*>	Optional. Displays DHCP information for the client using the specified interface.
ip <*ip address*>	Optional. Displays DHCP information for the client at the specified IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
mac <*mac address*>	Optional. Displays DHCP information for the client at the specified medium access control (MAC) address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following is sample output from the **show network-forensics ip dhcp** command:

```
#show network-forensics ip dhcp
Client MAC/IP/Host: 00:E0:29:0E:D5:E3 / 10.23.220.1 / xpsp3-host
    VLAN ID: 100
    Source Port: gigabit-switchport 0/2
    Server Mac/IP: 00:E0:29:0E:D5:E5 / 10.23.220.254
    Lease from Time Collected: 3 days from 25 Aug 2009 10:33:42
    Client Vendor Class: unknown
```

The preceding output is for one client. This same information will be displayed for all connected clients unless one of the filtering parameters is used in conjunction with the ***show network-forensics ip dhcp*** *command.*

show network-sync

Use the **show network-sync** command to display the status of the network synchronization (Network Sync) configuration. Variations of this command include:

show network-sync
show network-sync detail

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Optional. Displays details about the configuration.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example displays the status of the Network Sync configuration:

```
>enable
#show network-sync
Network Sync Status
Primary Source              gigabit-ethernet 0/1
    Health                  Down
Secondary Source            gigabit-ethernet 0/2
    Health                  Down
Current Source              Holdover
Revertive Mode              Priority
EEC Option                  EEC Option 1
ESMC Process                Enabled
Holdover Threshold          Threshold Holdover when clock source SSM < QL-EEC1
```


show ntp associations

Use the **show ntp associations** command to display the active Network Time Protocol (NTP) associations.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example executes **show ntp associations**:

```
>enable
#show ntp associations
```


show ntp status

Use the **show ntp status** command to display general information about the status on the Network Time Protocol (NTP).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example executes **show ntp status**:

```
>enable
#show ntp status
```


show ospfv3

Use the **show ospfv3** command to display general information regarding Open Shortest Path First version 3 (OSPFv3) processes on the AOS device. Variations of this command include:

show ospfv3

show ospfv3 *<process id>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from this command:

```
>enable
#show ospfv3
Summary of OSPFv3 Process 61 with ID: 5.5.5.5, VRF RED
  Supports IPv6 Address Family
  SPF delay timer: 5 seconds, Hold time between SPFs: 10 seconds
  LSA interval: 1800 seconds
  Number of external LSAs: 4, Checksum Sum: 0x22a04
  Number of AS scoped unknown LSAs: 0, Checksum Sum: 0x0
  Number of areas: 2, normal: 2, stub: 0, NSSA: 0
  Reference bandwidth unit is 100 Mbps
    Area (0) 5.5.5.5
      Number of interfaces in this area: 2
      Authentication type: 0
      SPF algorithm execution count: 2
      Number of LSAs: 8, Checksum Sum: 0x3f91a
    Area (1) 5.5.5.5
```



```
    Number of interfaces in this area: 1
   Authentication type: 0
    SPF algorithm execution count: 3
    Number of LSAs: 6, Checksum Sum: 0x39601
```


show ospfv3 database

Use the **show ospfv3 database** command to display information contained in the Open Shortest Path First version 3 (OSPFv3) link state database. Variations of this command include:

show ospfv3 database
show ospfv3 database adv-router *<router id>*
show ospfv3 database database-summary
show ospfv3 *<process id>* **database**
show ospfv3 *<process id>* **database adv-router** *<router id>*
show ospfv3 *<process id>* **database database-summary**
show ospfv3 *<process id>* *<area id>* **database**
show ospfv3 *<process id>* *<area id>* **database adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database database-summary**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.
database-summary	Optional. Displays summarized information about the OSPFv3 link state database.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database** command:

```
>enable
#show ospfv3 database
OSPFv3 router with ID: 4.4.4.4 (Process ID 61, VRF RED)

  Router Link States, Area 0
  Adv Router      Age      Seq #       Fragment ID  Link count   Bits
   4.4.4.4        222      0x8000005A  0            1            B, E
   5.5.5.5        215      0x80000066  0            1            B, E

  Network Link States, Area 0
  Adv Router      Age      Seq #       Link ID    Rtr count
   4.4.4.4        225      0x80000001  8          2

  Inter Area Prefix Link States, Area 0
  Adv Router      Age      Seq #       Prefix
   4.4.4.4        595      0x80000057  2001:10:24:204::/64
   5.5.5.5        220      0x80000001  2001:10:24:205::/64

  Link (Type-8) Link States, Area 0
  Adv Router      Age      Seq#        Link ID    Interface
   4.4.4.4        595      0x80000057  8          eth 0/1.106
   5.5.5.5        220      0x80000062  13         eth 0/1.106

  Intra Area Prefix Link States, Area 0
  Adv Router      Age      Seq #       Link ID    Ref-lstype  Ref-LSID
   4.4.4.4        225      0x80000001  8192       0x2002      8

  Router Link States, Area 1
  Adv Router      Age      Seq #       Fragment ID  Link count   Bits
   5.5.5.5        183      0x80000003  0            0            B, E

  Inter Area Prefix Link States, Area 1
  Adv Router      Age      Seq #       Prefix
   5.5.5.5        220      0x80000001  2001:10:24:106::/64
   5.5.5.5        211      0x80000001  2001:10:24:204::/64

  Inter Area Router Link States, Area 1
  Adv Router      Age      Seq #       Ref-router
   5.5.5.5        211      0x80000001  4.4.4.4

  Link (Type-8) Link States, Area 1
  Adv Router      Age      Seq#        Link ID    Interface
   5.5.5.5        223      0x80000001  14         eth 0/2.1
```

```
 Intra Area Prefix Link States, Area 1
  Adv Router      Age      Seq #       Link ID    Ref-lstype  Ref-LSID
  5.5.5.5         183      0x80000003  0          0x2001      0

 External Link States
  Adv Router      Age      Seq #       Prefix
  4.4.4.4         595      0x80000057  2001:7:1::/64
  4.4.4.4         595      0x80000057  2001:10:24:202::/64
  5.5.5.5         223      0x80000001  2001:8:1::/64
  5.5.5.5         223      0x80000001  2001:8:2::/64
```

The following is sample output from the **show ospfv3 database database-summary** command:

```
>enable
#show ospfv3 database database-summary
OSPFv3 router with ID: 5.5.5.5 (Process ID 61, VRF RED)
Area 0 database summary
    LSA Type          Count
    Router            2
    Network           1
    Link              2
    Prefix            1
    Inter-area Prefix 2
    Inter-area Router 0
    Unknown           0
    Subtotal          8
    External          4
    AS Unknown        0

Area 1 database summary
    LSA Type          Count
    Router            1
    Network           0
    Link              1
    Prefix            1
    Inter-area Prefix 2
    Inter-area Router 1
    Unknown           0
    Subtotal          6
    External          4
    AS Unknown        0
```

show ospfv3 database external

Use the **show ospfv3 database external** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of external link state advertisements (LSAs). Variations of this command include:

show ospfv3 database external
show ospfv3 database external *<ipv6 address/prefix-length>*
show ospfv3 database external *<ipv6 address/prefix-length> <link state id>*
show ospfv3 database external *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>*
show ospfv3 database external *<link state id>*
show ospfv3 database external *<link state id>* **adv-router** *<router id>*
show ospfv3 database external adv-router *<router id>*
show ospfv3 *<process id>* **database external**
show ospfv3 *<process id>* **database external** *<ipv6 address/prefix-length>*
show ospfv3 *<process id>* **database external** *<ipv6 address/prefix-length> <link state id>*
show ospfv3 *<process id>* **database external** *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database external** *<link state id>*
show ospfv3 *<process id>* **database external** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database external adv-router** *<router id>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<ipv6 address/prefix-length>	Optional. Limits the output of this command to a single Internet Protocol version 6 (IPv6) address. Enter IPv6 addresses in colon hexadecimal format (**X:X:X:X::X/<Z>**), for example, **2001:DB8::1/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<link state id>	Optional. Limits the output of this command to a single specified LSA.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database external** command:

```
>enable
#show ospfv3 database external
External Link States

   Link State age: 689
   Link State type: AS External-LSA (0x4005)
   Link State ID: 0
   Advertising Router: 4.4.4.4
   Sequence Number: 0x80000057
   Checksum: 0xBE61
   Length: 36
     Prefix Address: 2001:7:1::
     Prefix Length: 64, Options: None
     Metric Type: 1 (Comparable directly to link state metric)
     Metric: 22222

   Link State age: 689
   Link State type: AS External-LSA (0x4005)
   Link State ID: 1
   Advertising Router: 4.4.4.4
   Sequence Number: 0x80000057
   Checksum: 0xAB43
   Length: 36
     Prefix Address: 2001:10:24:202::
     Prefix Length: 64, Options: None
     Metric Type: 1 (Comparable directly to link state metric)
     Metric: 22222

   Link State age: 317
   Link State type: AS External-LSA (0x4005)
   Link State ID: 2
   Advertising Router: 5.5.5.5
   Sequence Number: 0x80000001
   Checksum: 0x5D34
   Length: 52
     Prefix Address: 2001:8:1::
     Prefix Length: 64, Options: None
     Metric Type: 1 (Comparable directly to link state metric)
     Metric: 11111
     Forwarding Address: 2001:10:24:205::2
```

```
Link State age: 317
Link State type: AS External-LSA (0x4005)
Link State ID: 3
Advertising Router: 5.5.5.5
Sequence Number: 0x80000001
Checksum: 0x632C
Length: 52
  Prefix Address: 2001:8:2::
  Prefix Length: 64, Options: None
  Metric Type: 1 (Comparable directly to link state metric)
  Metric: 11111
  Forwarding Address: 2001:10:24:205::2
```

show ospfv3 database inter-area prefix

Use the **show ospfv3 database inter-area prefix** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of inter-area prefix link state advertisements (LSAs). Variations of this command include:

show ospfv3 database inter-area prefix
show ospfv3 database inter-area prefix *<ipv6 address/prefix-length>*
show ospfv3 database inter-area prefix *<ipv6 address/prefix-length> <link state id>*
show ospfv3 database inter-area prefix *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>*
show ospfv3 database inter-area prefix *<link state id>*
show ospfv3 database inter-area prefix *<link state id>* **adv-router** *<router id>*
show ospfv3 database inter-area prefix adv-router *<router id>*
show ospfv3 *<process id>* **database inter-area prefix**
show ospfv3 *<process id>* **database inter-area prefix** *<ipv6 address/prefix-length>*
show ospfv3 *<process id>* **database inter-area prefix** *<ipv6 address/prefix-length> <link state id>*
show ospfv3 *<process id>* **database inter-area prefix** *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database inter-area prefix** *<link state id>*
show ospfv3 *<process id>* **database inter-area prefix** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database inter-area prefix adv-router** *<router id>*
show ospfv3 *<process id> <area id>* **database inter-area prefix**
show ospfv3 *<process id> <area id>* **database inter-area prefix** *<ipv6 address/prefix-length>*
show ospfv3 *<process id> <area id>* **database inter-area prefix** *<ipv6 address/prefix-length> <link state id>*
show ospfv3 *<process id> <area id>* **database inter-area prefix** *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>*
show ospfv3 *<process id> <area id>* **database inter-area prefix** *<link state id>*
show ospfv3 *<process id> <area id>* **database inter-area prefix** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id> <area id>* **database inter-area prefix adv-router** *<router id>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.

<ipv6 address/prefix-length>	Optional. Limits the output of this command to a single Internet Protocol version 6 (IPv6) address. Enter IPv6 addresses in colon hexadecimal format (**X:X:X:X::X/**<**Z**>), for example, **2001:DB8::1/64**. The prefix length (<**Z**>) is an integer with a value between **0** and **128**.
<link state id>	Optional. Limits the output of this command to a single specified LSA.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database inter-area prefix** command:

```
>enable
#show ospfv3 database inter-area prefix
OSPFv3 router with ID: 4.4.4.4 (Process ID 61, VRF RED)

  Inter Area Prefix Link States, Area 0

    Link State age: 728
    Link State type: Inter-Area-Prefix-LSA (0x2003)
    Link State ID: 0
    Advertising Router: 4.4.4.4
    Sequence Number: 0x80000057
    Checksum: 0x55DE
    Length: 36
      Metric: 1
      Prefix Address: 2001:10:24:204::
      Prefix Length: 64, Options: None

    Link State age: 353
    Link State type: Inter-Area-Prefix-LSA (0x2003)
    Link State ID: 1
    Advertising Router: 5.5.5.5
    Sequence Number: 0x80000001
    Checksum: 0xEB98
    Length: 36
      Metric: 1
      Prefix Address: 2001:10:24:205::
      Prefix Length: 64, Options: None

  Inter Area Prefix Link States, Area 1
```



```
Link State age: 353
Link State type: Inter-Area-Prefix-LSA (0x2003)
Link State ID: 2
Advertising Router: 5.5.5.5
Sequence Number: 0x80000001
Checksum: 0xE2A0
Length: 36
  Metric: 1
  Prefix Address: 2001:10:24:106::
  Prefix Length: 64, Options: None

Link State age: 344
Link State type: Inter-Area-Prefix-LSA (0x2003)
Link State ID: 4
Advertising Router: 5.5.5.5
Sequence Number: 0x80000001
Checksum: 0xBBC6
Length: 36
  Metric: 1
  Prefix Address: 2001:10:24:204::
  Prefix Length: 64, Options: None
```

show ospfv3 database inter-area router

Use the **show ospfv3 database inter-area router** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of inter-area router link state advertisements (LSAs). Variations of this command include:

show ospfv3 database inter-area router
show ospfv3 database inter-area router internal
show ospfv3 database inter-area router *<ipv6 address/prefix-length>*
show ospfv3 database inter-area router *<ipv6 address/prefix-length>* **internal**
show ospfv3 database inter-area router *<ipv6 address/prefix-length> <link state id>*
show ospfv3 database inter-area router *<ipv6 address/prefix-length> <link state id>* **internal**
show ospfv3 database inter-area router *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>*
show ospfv3 database inter-area router *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>* **internal**
show ospfv3 database inter-area router *<link state id>*
show ospfv3 database inter-area router *<link state id>* **internal**
show ospfv3 database inter-area router *<link state id>* **adv-router** *<router id>*
show ospfv3 database inter-area router *<link state id>* **adv-router** *<router id>* **internal**
show ospfv3 database inter-area router adv-router *<router id>*
show ospfv3 database inter-area router adv-router *<router id>* **internal**
show ospfv3 *<process id>* **database inter-area router**
show ospfv3 *<process id>* **database inter-area router internal**
show ospfv3 *<process id>* **database inter-area router** *<ipv6 address/prefix-length>*
show ospfv3 *<process id>* **database inter-area router** *<ipv6 address/prefix-length>* **internal**
show ospfv3 *<process id>* **database inter-area router** *<ipv6 address/prefix-length> <link state id>*
show ospfv3 *<process id>* **database inter-area router** *<ipv6 address/prefix-length> <link state id>* **internal**
show ospfv3 *<process id>* **database inter-area router** *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database inter-area router** *<ipv6 address/prefix-length> <link state id>* **adv-router** *<router id>* **internal**
show ospfv3 *<process id>* **database inter-area router** *<link state id>*
show ospfv3 *<process id>* **database inter-area router** *<link state id>* **internal**
show ospfv3 *<process id>* **database inter-area router** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database inter-area router** *<link state id>* **adv-router** *<router id>* **internal**
show ospfv3 *<process id>* **database inter-area router adv-router** *<router id>*
show ospfv3 *<process id>* **database inter-area router adv-router** *<router id>* **internal**
show ospfv3 *<process id> <area id>* **database inter-area router**
show ospfv3 *<process id> <area id>* **database inter-area router internal**
show ospfv3 *<process id> <area id>* **database inter-area router** *<ipv6 address/prefix-length>*
show ospfv3 *<process id> <area id>* **database inter-area router** *<ipv6 address/prefix-length>* **internal**
show ospfv3 *<process id> <area id>* **database inter-area router** *<ipv6 address/prefix-length> <link state id>*

show ospfv3 *<process id>* *<area id>* **database inter-area router** *<ipv6 address/prefix-length>* *<link state id>* **internal**
show ospfv3 *<process id>* *<area id>* **database inter-area router** *<ipv6 address/prefix-length>* *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database inter-area router** *<ipv6 address/prefix-length>* *<link state id>* **adv-router** *<router id>* **internal**
show ospfv3 *<process id>* *<area id>* **database inter-area router** *<link state id>*
show ospfv3 *<process id>* *<area id>* **database inter-area router** *<link state id>* **internal**
show ospfv3 *<process id>* *<area id>* **database inter-area router** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database inter-area router** *<link state id>* **adv-router** *<router id>* **internal**
show ospfv3 *<process id>* *<area id>* **database inter-area router adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database inter-area router adv-router** *<router id>* **internal**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
<ipv6 address/prefix-length>	Optional. Limits the output of this command to a single Internet Protocol version 6 (IPv6) address. Enter IPv6 addresses in colon hexadecimal format (**X:X:X:X::X/<Z>**), for example, **2001:DB8::1/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<link state id>	Optional. Limits the output of this command to a single specified LSA.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.
internal	Optional. Displays the shortest path first (SPF) calculation results for the LSAs and whether the LSA was used in route calculation.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database inter-area router** command:

```
>enable
#show ospfv3 database inter-area router

OSPFv3 router with ID: 5.5.5.5 (Process ID 61, VRF RED)

  Inter Area Router Link States, Area 1

    Link State age: 394
    Link State type: Inter-Area-Prefix-LSA (0x2004)
    Link State ID: 3
    Advertising Router: 5.5.5.5
    Sequence Number: 0x80000001
    Checksum: 0x37C6
    Length: 32
      Options: V6, E, R, AF
      Metric: 1
      Destination Router: 4.4.4.4
```


show ospfv3 database link

Use the **show ospfv3 database link** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of link state advertisements (LSAs). Variations of this command include:

show ospfv3 database link
show ospfv3 database link interface *<interface>*
show ospfv3 database link interface *<interface>* *<link state id>*
show ospfv3 database link interface *<interface>* *<link state id>* **adv-router** *<router id>*
show ospfv3 database link interface *<interface>* **adv-router** *<router id>*
show ospfv3 database link interface [mef-ethernet *<slot/port>* **| system-control-evc | system-management-evc]**
show ospfv3 database link interface [mef-ethernet *<slot/port>* **| system-control-evc | system-management-evc]** *<link state id>*
show ospfv3 database link interface [mef-ethernet *<slot/port>* **| system-control-evc | system-management-evc]** *<link state id>* **adv-router** *<router id>*
show ospfv3 database link interface [mef-ethernet *<slot/port>* **| system-control-evc | system-management-evc] adv-router** *<router id>*
show ospfv3 database link *<link state id>*
show ospfv3 database link *<link state id>* **adv-router** *<router id>*
show ospfv3 database link adv-router *<router id>*
show ospfv3 *<process id>* **database link**
show ospfv3 *<process id>* **database link interface** *<interface>*
show ospfv3 *<process id>* **database link interface** *<interface>* *<link state id>*
show ospfv3 *<process id>* **database link interface** *<interface>* *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database link interface** *<interface>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc]**
show ospfv3 *<process id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc]** *<link state id>*
show ospfv3 *<process id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc]** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc] adv-router** *<router id>*
show ospfv3 *<process id>* **database link** *<link state id>*
show ospfv3 *<process id>* **database link** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database link adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database link**
show ospfv3 *<process id>* *<area id>* **database link interface** *<interface>*
show ospfv3 *<process id>* *<area id>* **database link interface** *<interface>* *<link state id>*
show ospfv3 *<process id>* *<area id>* **database link interface** *<interface>* *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database link interface** *<interface>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc]**
show ospfv3 *<process id>* *<area id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc]** *<link state id>*

show ospfv3 *<process id>* *<area id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc]** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database link interface [mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc] adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database link** *<link state id>*
show ospfv3 *<process id>* *<area id>* **database link** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database link adv-router** *<router id>*

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
interface *<interface>*	Optional. Limits the output of this command to a single OSPFv3 interface. Specify interfaces in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id>*. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. Enter **show ipv6 ospfv3 database link interface ?** for a list of available interfaces.
mef-ethernet *<slot/port>*	Optional. Limits the output of this command to the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Limits the output of this command to the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Limits the output of this command to the system management EVC.
<link state id>	Optional. Limits the output of this command to a single specified LSA.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Usage Examples

The following is sample output from the **show ospfv3 database link** command:

```
>enable
#show ospfv3 database link
OSPFv3 router with ID: 4.4.4.4 (Process ID 61, VRF RED)

  Link (Type-8) Link States, Area 0

    Link State age: 813
    Link State type: Link-LSA (Interface: eth 0/1.106) (0x0008)
    Link State ID: 8
    Advertising Router: 4.4.4.4
    Sequence Number: 0x80000057
    Checksum: 0xEFB2
    Length: 56
      Options: V6, E, R, DC
      Router Priority: 1
      Link-Local Address: FE80::CA9C:1DFF:FED6:E0A0
      Number of Prefixes: 1
        Prefix Address: 2001:10:24:106::
        Prefix Length: 64, Options: None

    Link State age: 438
    Link State type: Link-LSA (Interface: eth 0/1.106) (0x0008)
    Link State ID: 13
    Advertising Router: 5.5.5.5
    Sequence Number: 0x80000062
    Checksum: 0xCD3
    Length: 56
      Options: V6, E, R, AF
      Router Priority: 1
      Link-Local Address: FE80::2A0:C8FF:FE1F:CC53
      Number of Prefixes: 1
        Prefix Address: 2001:10:24:106::
        Prefix Length: 64, Options: None

  Link (Type-8) Link States, Area 1

    Link State age: 441
```

```
Link State type: Link-LSA (Interface: eth 0/2.1) (0x0008)
Link State ID: 14
Advertising Router: 5.5.5.5
Sequence Number: 0x80000001
Checksum: 0xD965
Length: 56
  --MORE--
```

show ospfv3 database network

Use the **show ospfv3 database network** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of network link state advertisements (LSAs). Variations of this command include:

show ospfv3 database network
show ospfv3 database network *<link state id>*
show ospfv3 database network *<link state id>* **adv-router** *<router id>*
show ospfv3 database network adv-router *<router id>*
show ospfv3 *<process id>* **database network**
show ospfv3 *<process id>* **database network** *<link state id>*
show ospfv3 *<process id>* **database network** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database network adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database network**
show ospfv3 *<process id>* *<area id>* **database network** *<link state id>*
show ospfv3 *<process id>* *<area id>* **database network** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database network adv-router** *<router id>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
<link state id>	Optional. Limits the output of this command to a single specified LSA.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database network** command:

```
>enable
#show ospfv3 database network
OSPFv3 router with ID: 4.4.4.4 (Process ID 61, VRF RED)

  Network Link States, Area 0

    Link State age: 471
    Link State type: Network-LSA (0x2002)
    Link State ID: 8
    Advertising Router: 4.4.4.4
    Sequence Number: 0x80000001
    Checksum: 0xB01B
    Length: 32
      Options: V6, E, R, DC, AF
      Number of Attached Routers: 2
        Attached Router: 4.4.4.4
        Attached Router: 5.5.5.5
```


show ospfv3 database prefix

Use the **show ospfv3 database prefix** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of intra-area link state advertisements (LSAs). Variations of this command include:

show ospfv3 database prefix
show ospfv3 database prefix ref-lsa network
show ospfv3 database prefix ref-lsa network *<link state id>*
show ospfv3 database prefix ref-lsa network *<link state id>* **adv-router** *<router id>*
show ospfv3 database prefix ref-lsa network adv-router *<router id>*
show ospfv3 database prefix ref-lsa router
show ospfv3 database prefix ref-lsa router *<link state id>*
show ospfv3 database prefix ref-lsa router *<link state id>* **adv-router** *<router id>*
show ospfv3 database prefix ref-lsa router adv-router *<router id>*
show ospfv3 *<process id>* **database prefix**
show ospfv3 *<process id>* **database prefix ref-lsa network**
show ospfv3 *<process id>* **database prefix ref-lsa network** *<link state id>*
show ospfv3 *<process id>* **database prefix ref-lsa network** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database prefix ref-lsa network adv-router** *<router id>*
show ospfv3 *<process id>* **database prefix ref-lsa router**
show ospfv3 *<process id>* **database prefix ref-lsa router** *<link state id>*
show ospfv3 *<process id>* **database prefix ref-lsa router** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database prefix ref-lsa router adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database prefix**
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa network**
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa network** *<link state id>*
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa network** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa network adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa router**
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa router** *<link state id>*
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa router** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database prefix ref-lsa router adv-router** *<router id>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
<link state id>	Optional. Limits the output of this command to a single specified LSA.
ref-lsa	Optional. Limits the output of this command to all referenced LSAs.
network	Optional. Limits the output of this command to referenced network LSAs.
router	Optional. Limits the output of this command to referenced router LSAs.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database prefix** command:

```
>enable
#show ospfv3 database prefix
OSPFv3 router with ID: 4.4.4.4 (Process ID 61, VRF RED)

  Intra Area Prefix Link States, Area 0

    Link State age: 539
    Link State type: Intra-Area-Prefix-LSA (0x2009)
    Link State ID: 8192
    Advertising Router: 4.4.4.4
    Sequence Number: 0x80000001
    Checksum: 0x1809
    Length: 44
      Referenced LSA Type: 0x2002
      Referenced Link State ID: 8
      Referenced Advertising Router: 4.4.4.4
      Number of Prefixes: 1
        Prefix Address: 2001:10:24:106::
        Prefix Length: 64, Options: None, Metric: 0

  Intra Area Prefix Link States, Area 1

    Link State age: 497
```



```
Link State type: Intra-Area-Prefix-LSA (0x2009)
Link State ID: 0
Advertising Router: 5.5.5.5
Sequence Number: 0x80000003
Checksum: 0x44FA
Length: 44
  Referenced LSA Type: 0x2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 5.5.5.5
  Number of Prefixes: 1
    Prefix Address: 2001:10:24:205::
    Prefix Length: 64, Options: None, Metric: 1
```

show ospfv3 database router

Use the **show ospfv3 database router** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of router link state advertisements (LSAs). Variations of this command include:

show ospfv3 database router
show ospfv3 database router internal
show ospfv3 database router *<link state id>*
show ospfv3 database router *<link state id>* **internal**
show ospfv3 database router *<link state id>* **adv-router** *<router id>*
show ospfv3 database router *<link state id>* **adv-router** *<router id>* **internal**
show ospfv3 database router adv-router *<router id>*
show ospfv3 database router adv-router *<router id>* **internal**
show ospfv3 *<process id>* **database router**
show ospfv3 *<process id>* **database router internal**
show ospfv3 *<process id>* **database router** *<link state id>*
show ospfv3 *<process id>* **database router** *<link state id>* **internal**
show ospfv3 *<process id>* **database router** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* **database router** *<link state id>* **adv-router** *<router id>* **internal**
show ospfv3 *<process id>* **database router adv-router** *<router id>*
show ospfv3 *<process id>* **database router adv-router** *<router id>* **internal**
show ospfv3 *<process id>* *<area id>* **database router**
show ospfv3 *<process id>* *<area id>* **database router internal**
show ospfv3 *<process id>* *<area id>* **database router** *<link state id>*
show ospfv3 *<process id>* *<area id>* **database router** *<link state id>* **internal**
show ospfv3 *<process id>* *<area id>* **database router** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database router** *<link state id>* **adv-router** *<router id>* **internal**
show ospfv3 *<process id>* *<area id>* **database router adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database router adv-router** *<router id>* **internal**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
<link state id>	Optional. Limits the output of this command to a single specified LSA.

adv-router <*router id*>	Optional. Limits the output of this command to a single specified advertising router.
internal	Optional. Displays the shortest path first (SPF) calculation results for the LSAs and whether the LSA was used in route calculation.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database router** command:

```
>enable
#show ospfv3 database router
OSPFv3 router with ID: 4.4.4.4 (Process ID 61, VRF RED)

  Router Link States, Area 0

    Link State age: 575
    Link State type: Router-LSA (0x2001)
    Link State ID: 0
    Advertising Router: 4.4.4.4
    Sequence Number: 0x8000005A
    Checksum: 0x4F23
    Length: 40
      Options: V6, E, R, DC
      Flags: Area Border Router, AS Boundary Router
      Number of Links: 1
        Link connected to: Transit network Link
          Link Metric: 1
          Local Interface ID: 8
          Neighbor (DR) Interface ID: 8
          Neighbor (DR) Router ID: 4.4.4.4

    Link State age: 568
    Link State type: Router-LSA (0x2001)
    Link State ID: 0
    Advertising Router: 5.5.5.5
    Sequence Number: 0x80000066
    Checksum: 0xA3D8
    Length: 40
      Options: V6, E, R, AF
      Flags: Area Border Router, AS Boundary Router
      Number of Links: 1
```



```
    Link connected to: Transit network Link
      Link Metric: 1
      Local Interface ID: 13
      Neighbor (DR) Interface ID: 8
      Neighbor (DR) Router ID: 4.4.4.4

  Router Link States, Area 1

    Link State age: 536
    Link State type: Router-LSA (0x2001)
    Link State ID: 0
    Advertising Router: 5.5.5.5
    Sequence Number: 0x80000003
    Checksum: 0xA176
    Length: 24
      Options: V6, E, R, AF
      Flags: Area Border Router, AS Boundary Router
      Number of Links: 0
```

show ospfv3 database unknown

Use the **show ospfv3 database unknown** command to display details from the Open Shortest Path First version 3 (OSPFv3) link state database of unknown link state advertisements (LSAs). Variations of this command include:

show ospfv3 database unknown
show ospfv3 database unknown as
show ospfv3 database unknown area
show ospfv3 database unknown link
show ospfv3 database unknown <*link state id*>
show ospfv3 database unknown <*link state id*> **as**
show ospfv3 database unknown <*link state id*> **area**
show ospfv3 database unknown <*link state id*> **link**
show ospfv3 database unknown <*link state id*> **adv-router** <*router id*>
show ospfv3 database unknown <*link state id*> **adv-router** <*router id*> **as**
show ospfv3 database unknown <*link state id*> **adv-router** <*router id*> **area**
show ospfv3 database unknown <*link state id*> **adv-router** <*router id*> **link**
show ospfv3 database unknown adv-router <*router id*>
show ospfv3 database unknown adv-router <*router id*> **as**
show ospfv3 database unknown adv-router <*router id*> **area**
show ospfv3 database unknown adv-router <*router id*> **link**
show ospfv3 <*process id*> **database unknown**
show ospfv3 <*process id*> **database unknown as**
show ospfv3 <*process id*> **database unknown area**
show ospfv3 <*process id*> **database unknown link**
show ospfv3 <*process id*> **database unknown** <*link state id*>
show ospfv3 <*process id*> **database unknown** <*link state id*> **as**
show ospfv3 <*process id*> **database unknown** <*link state id*> **area**
show ospfv3 <*process id*> **database unknown** <*link state id*> **link**
show ospfv3 <*process id*> **database unknown** <*link state id*> **adv-router** <*router id*>
show ospfv3 <*process id*> **database unknown** <*link state id*> **adv-router** <*router id*> **as**
show ospfv3 <*process id*> **database unknown** <*link state id*> **adv-router** <*router id*> **area**
show ospfv3 <*process id*> **database unknown** <*link state id*> **adv-router** <*router id*> **link**
show ospfv3 <*process id*> **database unknown adv-router** <*router id*>
show ospfv3 <*process id*> **database unknown adv-router** <*router id*> **as**
show ospfv3 <*process id*> **database unknown adv-router** <*router id*> **area**
show ospfv3 <*process id*> **database unknown adv-router** <*router id*> **link**
show ospfv3 <*process id*> <*area id*> **database unknown**
show ospfv3 <*process id*> <*area id*> **database unknown as**
show ospfv3 <*process id*> <*area id*> **database unknown area**
show ospfv3 <*process id*> <*area id*> **database unknown link**
show ospfv3 <*process id*> <*area id*> **database unknown** <*link state id*>
show ospfv3 <*process id*> <*area id*> **database unknown** <*link state id*> **as**
show ospfv3 <*process id*> <*area id*> **database unknown** <*link state id*> **area**
show ospfv3 <*process id*> <*area id*> **database unknown** <*link state id*> **link**

show ospfv3 *<process id>* *<area id>* **database unknown** *<link state id>* **adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database unknown** *<link state id>* **adv-router** *<router id>* **as**
show ospfv3 *<process id>* *<area id>* **database unknown** *<link state id>* **adv-router** *<router id>* **area**
show ospfv3 *<process id>* *<area id>* **database unknown** *<link state id>* **adv-router** *<router id>* **link**
show ospfv3 *<process id>* *<area id>* **database unknown adv-router** *<router id>*
show ospfv3 *<process id>* *<area id>* **database unknown adv-router** *<router id>* **as**
show ospfv3 *<process id>* *<area id>* **database unknown adv-router** *<router id>* **area**
show ospfv3 *<process id>* *<area id>* **database unknown adv-router** *<router id>* **link**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
<link state id>	Optional. Limits the output of this command to a single specified LSA.
adv-router *<router id>*	Optional. Limits the output of this command to a single specified advertising router.
as	Optional. Filters the output of this command by unknown LSA autonomous systems (AS).
area	Optional. Filters the output of this command by unknown LSA areas.
link	Optional. Filters the output of this command by unknown LSA links.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 database unknown** command:

```
>enable
#show ospfv3 database unknown
OSPFv3 router with ID: 4.4.4.4 (Process ID 61, VRF RED)

  Unknown Link States, Area 603979776

    Link State age: 273
    Link State type: Unknown (0x3FFF)
    Link State ID: 1
    Advertising Router: 10.80.52.106
    Sequence Number: 0x808DE8B1
    Checksum: 0xF1AE
    Length: 40
      Scope: Link Local
```

show ospfv3 interface

Use the **show ospfv3 interface** command to display Open Shortest Path First version 3 (OSPFv3) information related to router interfaces. Variations of this command include:

show ospfv3 interface
show ospfv3 interface *<interface>*
show ospfv3 interface mef-ethernet *<slot/port>*
show ospfv3 interface system-control-evc
show ospfv3 interface system-management-evc
show ospfv3 *<process id>* **interface**
show ospfv3 *<process id>* **interface** *<interface>*
show ospfv3 *<process id>* **interface mef-ethernet** *<slot/port>*
show ospfv3 *<process id>* **interface system-control-evc**
show ospfv3 *<process id>* **interface system-management-evc**
show ospfv3 *<process id>* *<area id>* **interface**
show ospfv3 *<process id>* *<area id>* **interface** *<interface>*
show ospfv3 *<process id>* *<area id>* **interface mef-etherent** *<slot/port>*
show ospfv3 *<process id>* *<area id>* **interface system-control-evc**
show ospfv3 *<process id>* *<area id>* **interface system-management-evc**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<area id>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.
<interface>	Optional. Limits the output of this command to a single OSPFv3 interface. Specify interfaces in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id>*. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. Enter **show ospfv3 interface ?** for a list of available interfaces.
mef-ethernet *<slot/port>*	Optional. Limits the output of this command to the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Limits the output of this command to the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Limits the output of this command to the system management EVC.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Usage Examples

The following is sample output from the **show ospfv3 interface** command:

```
>enable
#show ospfv3 interface
eth 0/1.106 is UP
    Link Local Address FE80::2A0:C8FF:FE1F:CC53, Interface ID 13
    Area 0, Process ID 61, VRF RED, Instance ID 0, Router ID 5.5.5.5
     Area 1, Process ID 24, VRF RED, Instance ID 1, Router ID 5.5.5.5
    Network type Broadcast, Cost: 1
    Transmit delay is 1, State BDR, Priority 1
    Designated Router (ID) 4.4.4.4, local address FE80::CA9C:1DFF:FED6:E0A0
    Backup Designated Router (ID) 5.5.5.5, local address FE80::2A0:C8FF:FE1F:CC53
    Timer intervals configured, Hello 10, Dead 40, Retransmit 5
        Hello due in 00:00:04
     Neighbor Count is 1, Adjacent neighbors count is 1
        Adjacent with neighbor 4.4.4.4 (Designated Router)
    Suppress hello for 0 neighbor(s)
eth 0/2.1 is UP
    Link Local Address FE80::2A0:C8FF:FE1F:CC54, Interface ID 14
     Area 1, Process ID 61, Instance ID 0, Router ID 5.5.5.5
    Network type Broadcast, Cost: 1
    Transmit delay is 1, State DR, Priority 1
    Designated Router (ID) 5.5.5.5, local address FE80::2A0:C8FF:FE1F:CC54
    Backup Designated Router (ID) 0.0.0.0, local address ::
    Timer intervals configured, Hello 10, Dead 40, Retransmit 5
        Hello due in 00:00:06
    Neighbor Count is 0, Adjacent neighbors count is 0
    Suppress hello for 0 neighbor(s)
```

show ospfv3 neighbor

Use the **show ospfv3 neighbor** command to display Open Shortest Path First version 3 (OSPFv3) information related to OSPFv3 neighbors. Variations of this command include:

show ospfv3 neighbor
show ospfv3 neighbor detail
show ospfv3 neighbor <*interface*>
show ospfv3 neighbor <*interface*> **detail**
show ospfv3 neighbor <*interface*> **hostname**
show ospfv3 neighbor <*interface*> **hostname detail**
show ospfv3 neighbor <*interface*> <*router id*>
show ospfv3 neighbor <*interface*> <*router id*> **detail**
show ospfv3 neighbor hostname
show ospfv3 neighbor hostname detail
show ospfv3 neighbor [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc]**
show ospfv3 neighbor [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc] detail**
show ospfv3 neighbor [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc] hostname**
show ospfv3 neighbor [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc] hostname detail**
show ospfv3 neighbor [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc]** <*router id*>
show ospfv3 neighbor [mef-ethernet <*slot/port*> **| system-control-evc | system-management-evc]** <*router id*> **detail**
show ospfv3 neighbor <*router id*>
show ospfv3 neighbor <*router id*> **detail**
show ospfv3 <*process id*> **neighbor**
show ospfv3 <*process id*> **neighbor detail**
show ospfv3 <*process id*> **neighbor** <*interface*>
show ospfv3 <*process id*> **neighbor** <*interface*> **detail**
show ospfv3 <*process id*> **neighbor** <*interface*> **hostname**
show ospfv3 <*process id*> **neighbor** <*interface*> **hostname detail**
show ospfv3 <*process id*> **neighbor** <*interface*> <*router id*>
show ospfv3 <*process id*> **neighbor** <*interface*> <*router id*> **detail**
show ospfv3 <*process id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show ospfv3 <*process id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] detail**
show ospfv3 <*process id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] hostname**
show ospfv3 <*process id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] hostname detail**
show ospfv3 <*process id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]** <*router id*>

show ospfv3 <*process id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]** <*router id*> **detail**
show ospfv3 <*process id*> **neighbor hostname**
show ospfv3 <*process id*> **neighbor hostname detail**
show ospfv3 <*process id*> **neighbor** <*router id*>
show ospfv3 <*process id*> **neighbor** <*router id*> **detail**
show ospfv3 <*process id*> <*area id*> **neighbor**
show ospfv3 <*process id*> <*area id*> **neighbor detail**
show ospfv3 <*process id*> <*area id*> **neighbor** <*interface*>
show ospfv3 <*process id*> <*area id*> **neighbor** <*interface*> **detail**
show ospfv3 <*process id*> <*area id*> **neighbor** <*interface*> **hostname**
show ospfv3 <*process id*> <*area id*> **neighbor** <*interface*> **hostname detail**
show ospfv3 <*process id*> <*area id*> **neighbor** <*interface*> <*router id*>
show ospfv3 <*process id*> <*area id*> **neighbor** <*interface*> <*router id*> **detail**
show ospfv3 <*process id*> <*area id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]**
show ospfv3 <*process id*> <*area id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] detail**
show ospfv3 <*process id*> <*area id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] hostname**
show ospfv3 <*process id*> <*area id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc] hostname detail**
show ospfv3 <*process id*> <*area id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]** <*router id*>
show ospfv3 <*process id*> <*area id*> **neighbor [mef-ethernet** <*slot/port*> **| system-control-evc | system-management-evc]** <*router id*> **detail**
show ospfv3 <*process id*> <*area id*> **neighbor hostname**
show ospfv3 <*process id*> <*area id*> **neighbor hostname detail**
show ospfv3 <*process id*> <*area id*> **neighbor** <*router id*>
show ospfv3 <*process id*> <*area id*> **neighbor** <*router id*> **detail**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*process id*>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.
<*area id*>	Optional. Limits the output of this command to a single OSPFv3 area. Valid range is **0** to **4294967295**.

<interface>	Optional. Limits the output of this command to a single OSPFv3 interface. Specify interfaces in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id>*. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**. Enter **show ospfv3 neighbor ?** for a list of available interfaces.
mef-ethernet *<slot/port>*	Optional. Limits the output of this command to the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Limits the output of this command to the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Limits the output of this command to the system management EVC.
<router id>	Optional. Limits the output of this command to a single specified advertising router by router ID.
hostname	Optional. Limits the output of this command to a single specified router by router host name.
detail	Optional. Specifies that more detailed information is displayed in the command output.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Usage Examples

The following is sample output from the **show ospfv3 neighbor** command:

```
>enable
#show ospfv3 neighbor
OSPFv3 Router with ID (5.5.5.5) (Process ID 61, VRF RED)

Neighbor ID     Pri State           Dead Time  Intf-ID  Interface
4.4.4.4           1 FULL/DR         00:00:34      8     eth 0/1.106
```

show ospfv3 summary-prefix

Use the **show ospfv3 summary-prefix** command to display details about Open Shortest Path First version 3 (OSPFv3) redistributed routes that have been summarized using the command *summary-prefix <ipv6 address/prefix-length> on page 4166*. Variations of this command include:

show ospfv3 summary-prefix
show ospfv3 *<process id>* **summary-prefix**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<process id>	Optional. Limits the output of this command to a single OSPFv3 process. Valid range is **1** to **65535**.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following is sample output from the **show ospfv3 summary-prefix** command for process **61**:

```
>enable
#show ospfv3 61 summary-prefix
OSPFv3 Summary Addresses, Process ID 61, VRF RED:
  2001:8:7::/48 Metric 11111, Type 1, advertise
```


show output-chkdsk

Use the **show output-chkdsk** command to display output from the CFLASH checkdisk that occurs at boot up. File allocation table (FAT) errors detected or repaired are shown from the last boot up using this command. If checkdisk passed without incident, the command displays the output **File is empty**. This command is only applicable to Adtran integrated communications products (ICPs).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show output-chkdsk** command where checkdisk passed:

```
>enable
#show output-chkdsk
File is empty.
```

The following is sample output from the **show output-chkdsk** command where errors were detected and repaired. An explanation of the errors found follows the output:

```
>enable
#show output-chkdsk
## 'SystemDefaultPrompts' The '.' entry has a non-zero size (repaired).
## 'SystemDefaultPrompts' The '..' entry points to cluster 2 (should be root directory - repaired).
## Cluster 583 chains to 435, but 583 is already used in another chain.
## Terminated subsequent instance of cross-linked chain starting at 205 at cluster 394.
## 'VoiceMail' The '.' first entry was not found.
## 'VoiceMail' Found 2 checksum mismatches (repaired).
## 'VoiceMail/Messages' Found 3 trailing entries (repaired).
## 'VoiceMail' Found 2 duplicate entries (repaired).
```


The following errors are minor and can be ignored.

'SystemDefaultPrompts' The '.' entry has a non-zero size (repaired).
'SystemDefaultPrompts' The '..' entry points to cluster 2 (should be root directory - repaired).

The following errors are more serious, but have been repaired. They indicate that the FAT has been corrupted. In some instances, major files may be lost (if they were corrupt or were contained within a corrupt directory).

Found 20 orphaned clusters (not free and not used - repaired).
Cluster 583 chains to 435, but 583 is already used in another chain.
Terminated subsequent instance of cross-linked chain starting at 205 at cluster 394.

The following error results in the removal of the entire directory:

'VoiceMail' The '.' first entry was not found.

The following errors are minor. They indicate that some corruption has occurred, specifically with the naming units of the files involved. In most cases, these can be repaired without data loss.

'VoiceMail' Found 2 checksum mismatches (repaired).
'VoiceMail' Found 15 invalid names (repaired).
'VoiceMail/Messages' Found 3 trailing entries (repaired).
'VoiceMail' Found 2 duplicate entries (repaired).

show output-errors

Use the **show output-errors** command to display the startup error log. If no errors are encountered during startup, the command displays the output **File is empty**.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example shows output from the **show output-errors** command:

```
>enable
#show output-errors
File is empty.
```


show output-startup

Use the **show output-startup** command to display startup configuration output line by line. This output can be copied into a text file and then used as a configuration editing tool.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show output-startup** command:

```
>enable
#show output-startup
!
#!
#hostname "UNIT_2"
UNIT_2#no enable password
UNIT_2#!
UNIT_2#ip subnet-zero
UNIT_2#ip classless
UNIT_2#ip routing
UNIT_2#!
UNIT_2#event-history on
UNIT_2#no logging forwarding
UNIT_2#logging forwarding priority-level info
UNIT_2#no logging email
--MORE--
```


show over-temperature protection

Use the **show over-temperature protection** command to display current status for the over temperature protection feature.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.6.0	Command was introduced.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

The shutdown threshold is not user defined and cannot be changed on the unit. For more information about over temperature protection configuration, refer to the *Over-Temperature Protection Command Set on page 4446*.

This command is not available for vAOS instances.

Usage Examples

The following is sample output from the **show over-temperature protection** command:

```
>enable
#show over-temperature protection

    Over-Temperature Protection Status

    Admin State          : Enabled
    Warning Threshold    : 70C    158F
    Recovery Threshold   : 70C    158F
    Shutdown Threshold   : 75C    167F
```


show packet-capture

Use the **show packet-capture** command to display packet capturing statistics and verify the packet-capture configuration. Variations of this command include:

show packet-capture captures
show packet-capture captures memory-usage
show packet-capture captures memory-usage realtime
show packet-capture captures sip-calls
show packet-capture captures sip-calls realtime
show packet-capture captures realtime
show packet-capture interfaces
show packet-capture interfaces realtime
show packet-capture memory-usage
show packet-capture memory-usage captures
show packet-capture memory-usage captures realtime
show packet-capture memory-usage captures sip-calls
show packet-capture memory-usage captures sip-calls realtime
show packet-capture memory-usage interfaces
show packet-capture memory-usage interfaces realtime
show packet-capture memory-usage realtime
show packet-capture sip-calls
show packet-capture sip-calls realtime
show packet-capture
show packet-capture verbose realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

captures	Displays the active captures of every configured packet-capture.
interfaces	Displays the interfaces with attached packet-captures and any observed Netifs.
memory-usage	Displays packet capturing memory usage statistics. These statistics can be further limited by active captures, Session Initiation Protocol (SIP) calls, and interfaces.
sip-calls	Displays the active calls of every SIP packet-capture.
realtime	Optional. Displays the command output in realtime.
verbose	Optional. Displays detailed packet-capture information.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example displays the active captures of every configured packet-capture:

>**enable**
#show packet-capture captures
Active Captures:

CapturID	Packet-capture	State	Size	Start
331	1CAPTURE	open	24	2011.03.15 23:50:10
332	2CAPTURE	exporting	24	2011.03.15 23:48:27

Export Jobs (ongoing or recently completed):

CaptID	Sent	Destination	Status
332	151K	10.17.127.251:69	In progress

show port-auth

Use the **show port-auth** command to view port authentication information. Variations of this command include:

show port-auth
show port-auth detailed
show port-auth detailed interface <*interface*>
show port-auth interface <*interface*>
show port-auth statistics
show port-auth statistics interface <*interface*>
show port-auth summary
show port-auth summary interface <*interface*>
show port-auth supplicant
show port-auth supplicant interface <*interface*>
show port-auth supplicant summary
show port-auth supplicant summary interface <*interface*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detailed	Optional. Displays detailed port authentication information.
statistics	Optional. Displays port authentication statistics.
summary	Optional. Displays a summary of port authentication settings.
supplicant	Optional. Displays port authentication supplicant information.
interface <*interface*>	Optional. Displays port authentication information for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show port-auth interface ?** for a list of valid interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**, and the **supplicant** keyword.
Release A5.01	Command was expanded to include the Gigabit Ethernet and gigabit switchport interfaces.
Release R.11.5.0	Command was expanded to include media access control (MAC) authentication bypass information.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example displays the port authentication information:

```
>enable
#show port-auth
Global Port-Authentication Parameters:
   re-authentication enabled: False
   reauth-period: 3600
   quiet-period: 60
   tx-period: 30
   supp-timeout: 30
   server-timeout: 30
   reauth-max: 2
Port-Authentication Port Summary:
      * MAB - MAC Authentication Bypass
   Interface    Status       Type                Mode    Authorized
 ----------------------------------------------------------------------------------------------
   eth 0/1      disabled     port-based          n/a     n/a
   eth 0/2      disabled     port-based:MAB      auto    not authorized
   eth 0/3      disabled     port-based          n/a     n/a
   eth 0/4      disabled     port-based          n/a     n/a
   eth 0/5      disabled     port-based          n/a     n/a
   eth 0/6      disabled     port-based          n/a     n/a
   eth 0/7      disabled     port-based          n/a     n/a
   eth 0/8      disabled     port-based          n/a     n/a
   eth 0/9      disabled     port-based          n/a     n/a
   eth 0/10     disabled     port-based          n/a     n/a
   eth 0/11     disabled     port-based          n/a     n/a
   eth 0/12     disabled     port-based          n/a     n/a
   eth 0/13     disabled     port-based          n/a     n/a
   eth 0/14     disabled     port-based          n/a     n/a
   eth 0/15     disabled     port-based          n/a     n/a
   eth 0/16     disabled     port-based          n/a     n/a
   eth 0/17     disabled     port-based          n/a     n/a
   eth 0/18     disabled     port-based          n/a     n/a
```



```
  eth 0/19     disabled     port-based              n/a      n/a
Port Authentication Port Details:
  Port-Authentication is disabled on eth 0/1
  Port-Authentication is enabled on eth 0/2
    Status                    not authorized
    Auth Mode                 port-based
    Port-Control              auto
    Multiple Hosts Allowed    disabled
    MAC Auth Bypass           enabled
    Supplicant MAC            n/a
    Current Identifier        0
```

show port-security

Use the **show port-security** command to display port security information. Variations of this command include:

show port-security
show port-security address
show port-security interface *<interface>*
show port-security interface *<interface>* **address**
show port-security port-expiration
show port-security port-expiration detailed

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

address	Optional. Displays a list of secure medium access control (MAC) addresses for all interfaces currently configured for port security.
interface *<interface>*	Optional. Filters the output to include only information for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show port-security interface ?** for a complete list of valid interfaces.
port-expiration	Optional. Displays the ports currently participating in port expiration and the amount of time left until the port is shut down.
detailed	Optional. Displays information for all interfaces, even if not configured for port expiration.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 18.3	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following displays all secure MAC addresses related to the Ethernet 0/1 interface:

```
>enable
#show port-security interface eth 0/1 address
VLAN   Mac Address         Type of Entry     Interface   Remaining Time
-------------------------------------------------------------------------------------------------------------
1      00:a0:c8:0a:c6:4a   Dynamic-Secure    eth 0/1     --
1      00:a0:c8:0a:c6:4b   Dynamic-Secure    eth 0/1     --
-------------------------------------------------------------------------------------------------------------
Dynamic Address Count: 2
Static Address Count: 0
Sticky Address Count: 0
Total Address Count: 2
```

show power inline

Use the **show power inline** command to display power information (in watts) for devices connected to Power over Ethernet (PoE) interfaces. The command also displays the PoE interfaces that can be powered, whether the interfaces are powered or not, and the IEEE class for the device(s) connected to the PoE interfaces. Variations of this command include:

show power inline
show power inline <*slot/port*>
show power inline <*slot/port*> **realtime**
show power inline vcid <*vcid*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<*slot/port*>	Optional. Specifies the slot/port of a PoE interface. If specified, the command only displays information related to that interface.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.
vcid <*vcid*>	Optional. Specifies the virtual chassis ID of an ActivChassis member. If specified, the command only displays information related to that member. Valid VCID range is **1** to **8**. VCID values **1** and **2** are given to the ActivChassis master and backup devices, respectively.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 11.1	The **realtime** display parameter was added.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R10.7.0	Command was expanded to include the **vcid** parameter.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example displays power information for all PoE interfaces:

```
>enable
#show power inline
Interface       Admin       Oper       Power (watts)       Class
eth 0/1         auto        off        n/a                 n/a
eth 0/2         auto        off        n/a                 n/a
--MORE--
```


show power-supply

Use the **show power-supply** command to display the power supply status.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays the power supply status:

```
>enable
#show power-supply
Power supply 1 is OK.
Power supply 2 is not present.
```


show pppoe

Use the **show pppoe** command to display all Point-to-Point Protocol over Ethernet (PPPoE) settings and associated parameters.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example enters the Enable mode and uses the **show** command to display PPPoE information:

```
>enable
#show pppoe
ppp 1
 Outgoing Interface: eth 0/1
 Outgoing Interface MAC Address: 00:A0:C8:00:85:20
 Access-Concentrator Name Requested: FIRST VALID
 Access-Concentrator Name Received: 13021109813703-LRVLGAOS90W_IFITL
 Access-Concentrator MAC Address: 00:10:67:00:1D:B8
 Session Id: 64508
 Service Name Requested: ANY
 Service Name Available:
 PPPoE Client State: Bound (3)
 Redial retries: unlimited
 Redial delay: 10 seconds
Backup enabled all day on the following days:
    Sunday Monday Tuesday Wednesday Thursday Friday Saturday
```


show pppoe system-control-evc

Use the **show pppoe system-control-evc** command to display the Point-to-Point Protocol over Ethernet (PPPoE) settings for the system control Ethernet virtual connection (EVC).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No defaults are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display the PPPoE information for the system control EVC:

```
>enable
#show pppoe system-control-evc
```


show policer

Use the **show policer** command to display Ethernet virtual connection (EVC) traffic policer configuration and state information. Variations of this command include:

show policer

show policer *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Optional. Displays information about the connected EVC policer profile. If no name is specified, information for all policers is displayed.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display information for all configured EVC policers:

```
>enable
#show policer
Policer “policer1”
    Admin State          : Disabled
    Policer Status       : Disabled
    Configured CIR       : 0 kbps
    Configured EIR       : 600000 kbps
    Configured CBS       : 3125 bytes
    Configured EBS       : 12500 bytes
     Mode                : Not applied
```


show privilege

Use the **show privilege** command to display the current user's privilege level.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example displays the user's current privilege level as **1**:

```
>enable
#show privilege
Current privilege level is 1
```


show probe

Use the **show probe** command to display probe configuration and statistics. Refer to *Network Monitor Probe Command Set on page 4062* for information on configuring probe objects. Variations of this command include the following:

show probe
show probe <*name*>
show probe <*name*> **realtime**
show probe responder icmp-timestamp
show probe responder icmp-timestamp realtime
show probe responder twamp
show probe responder twamp realtime
show probe responder udp-echo
show probe responder udp-echo realtime
show probe <*name*> **statistics**
show probe <*name*> **statistics history**
show probe statistics
show probe statistics history

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<*name*>	Optional. Displays configuration and statistics for a specific probe.
responder	Displays the specified probe responder statistics.
icmp-timestamp	Optional. Displays the Internet Control Message Protocol (ICMP) timestamp probe responder statistics.
twamp	Optional. Displays the Two-Way Active Measurement Protocol (TWAMP) probe responder statistics.
udp-echo	Optional. Displays the User Datagram Protocol (UDP) echo probe responder statistics.
statistics	Optional. Displays measured probe statistics.
history	Optional. Displays the history of all measured probe statistics.

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.2	Command was expanded to include the probe responder options.
Release R13.5.0	Command output of **show udp echo** command was updated to include visibility of UDP echo probe responder hardware fast forwarding engine (FFE) support.

Functional Notes

A probe must be created first using the **probe** command. Issuing the shutdown command at the **probe** configuration prompt will disable a probe, causing it to cease traffic generation. While a probe is shutdown, it will not fail.

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Output from the **show probe responder udp-echo** command can vary depending on whether the hardware FFE feature is enabled or disabled on the AOS device. When hardware FFE is enabled, the **Rcvd** and **Sent** columns of the command output appear as **N/A**, and the **FFE Hits** and **Drops** columns of the output display current packet FFE and drop information. When hardware FFE is disabled, the command output displays current received (**Rcvd**) and sent (**Sent**) packet information and displays **N/A** for the **FFE Hits** and **Drops** columns.

Usage Examples

The following is sample output of the **show probe probe_A** command:

```
>enable
#show probe probe_A
Current State: PASS    Admin. Status: DOWN
    Type: ICMP Echo Period: 30 sec Timeout: 500 msec
    Hostname: www.adtran.com
    Tracked by: track_1
    Tests Run: 121 Failed: 0
    Time in current state: 25 days 2 hours, 34 minutes, 32 seconds
```


The following is sample output of the **show probe responder twamp** command:

```
>enable
#show probe responder twamp
0----------1----------2----------3----------4----------5----------6----------7----------8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
TWAMP-Test: 360 rcvd, 360 sent
TWAMP-Control: 20 sessions opened, 18 sessions closed,
        3 sessions rejected, 2 sessions active
```

The following is sample output of the **show probe responder icmp-timestamp** command:

```
>enable
#show probe responder icmp-timestamp
0----------1----------2----------3----------4----------5----------6----------7----------8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
ICMP Timestamp: 125 rcvd, 125 sent
```

The following is sample output of a TWAMP type probe named **Houston**:

```
>enable
#show probe Houston
0----------1----------2----------3----------4----------5----------6----------7----------8
12345678901234567890123456789012345678901234567890123456789012345678901234567890
Probe Houston:
 Current State: PASS Admin. Status: UP
 Type: TWAMP Period: 60 Timeout: 1500
 Source: 192.168.1.255:17001 Destination: 10.10.20.254:17000
 Data Size: 14 Num-packets 100 DSCP: 0
 Data pad: Zero
 Send-schedule: 20 msec Type: periodic
 Authentication Mode: open      Key: not set
 Tracked by: Nothing
 Tests Run: 194 Failed: 1
 Tolerance: not set
 Time in current state: 1 days, 2 hours, 50 minutes, 7 seconds
 Packet Loss          fail      pass
   Round Trip         1000      1000
```

The following is sample output of the **show probe responder udp-echo** command:

```
>enable
#show probe responder udp-echo
     Admin. Status: UP
     Rcvd     Sent     FFE Hits     Drops
     41       41       N/A          N/A
     N/A      N/A      19
```


show processes

Use the **show processes** command to display process statistic information. Variations of this command include:

show processes cpu
show processes cpu history
show processes cpu realtime
show processes history
show processes queue
show processes stack

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

cpu	Displays information about current active processes.
cpu history	Displays historical CPU utilization in graph form over the previous 1 minute, 1 hour, and 72 hour periods.
realtime	Displays full-screen CPU output in real time. Refer to the *Functional Notes* below for more information.
history	Displays process switch history.
queue	Displays process queue utilization.
stack	Displays the process stack usage.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 10.1	New option was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.5	Command was expanded to include the **stack** parameter.

Release R11.3.0	Command was expanded to include the **cpu history** parameter.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show processes cpu** command:

```
>enable
#show processes cpu
System load: 1sec:3.30%  1min:3.51%  5min:3.51%  Min: 0.00%  Max: 100.00%
Context switch load: 0.12%
```

Task Id	Task Name	PRI	STA	Invoked (count)	Exec Time (µsec)	Runtime (µsec)	Load %% (1sec)
1	Idle	0	W	116153	975	966830	96.68
3	PC Config	7	S	28509	8940	15347	1.53
4	PacketRouting	44	W	7418	7	1909	0.19
5	Timer	46	W	54628	12	1356	0.14
6	CallControlQue~	37	W	108	3	0	0.00
7	IsdnStackQueue	39	W	44	3	0	0.00
8	Thread Pool	4	W	45	204	0	0.00
9	con0	46	W	348	14	0	0.00
10	Driver Control	8	W	0	98	0	0.00
11	FrontPanel	43	W	8617	106	2189	0.22
12	eth01	46	W	2701	55	625	0.06
13	ICP Session	8	W	44	27	0	0.00

```
--MORE--
```

The following is sample output from the **show processes history** command:

```
>enable
#show processes history
CurrentTime     Task Name
---------------------------------------------
    9970752     PC Config
    9970752     FrontPanel
    9970752     TIDSPActiveQ
    9970752     Timer
    9970744     Idle
    9970744     FramerBaseThread
    9970744     FramerBaseThread
```



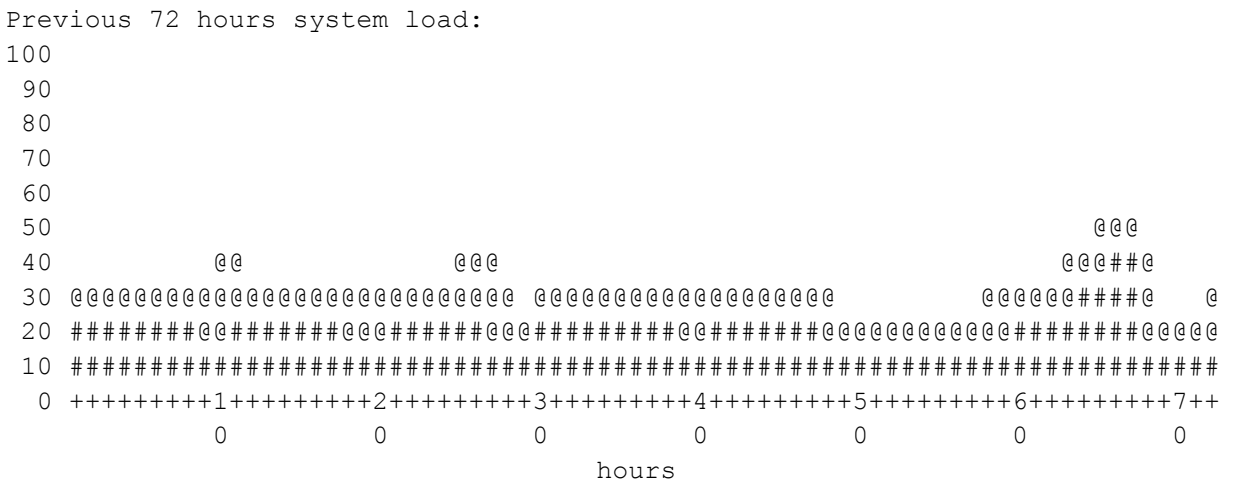
```
   9970744     FramerBaseThread
   9970744     FramerBaseThread
   9970741     Idle
   9970741     PCI Bridge
   9970735     Idle
   9970735     SnmpThread
   9970734     Idle
   9970734     FramerBaseThread
   9970734     FramerBaseThread
```

The following is sample output from the **show processes cpu history** command:

>**enable**
#show processes cpu history
#: Average load % per interval
@: Maximum load % per interval
Most current interval starts on the left.

```
Previous 1 minute system load:
100
 90
 80                                        ####
 70                                      ########
 60                                     #########
 50                                    ###########
 40                                  ################     #####
 30    ##    ##   ##########     ###################### ##########
 20  ############################################################
 10  ############################################################
  0 +++++++++1+++++++++2+++++++++3+++++++++4+++++++++5+++++++++6
             0         0         0         0         0         0
                               seconds


Previous 1 hour system load:
100
 90
 80
 70
 60
 50                 @         @@@                              @
 40           @@@@@@@@@@@@@@@@@@@@         @       @@@       @ @ @@
 30 @@@@@@@@@@##########@########@@ @@@@@@@@ @@@@@@@@ @  @@@ @ @@
 20 ################################################ @@@##########
 10 ############################################################
  0 +++++++++1+++++++++2+++++++++3+++++++++4+++++++++5+++++++++6
             0         0         0         0         0         0
                               minutes
```



show qos

Use the **show qos** command to display information regarding quality of service (QoS) and 802.1p class of service (CoS) settings. Variations of this command include:

show qos cos-map
show qos dscp-cos
show qos interface <*interface*>
show qos queuing

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

cos-map	Displays the CoS priority-to-queue map. The map outlines which CoS priority is associated with which queue.
dscp-cos	Displays the differentiated services code point (DSCP) to CoS map settings.
interface <*interface*>	Displays the configured values for default CoS and trust settings on a specific interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show qos interface ?** for a complete list of valid interfaces.
queuing	Displays the type of queuing being used. If weighted round robin (WRR) queuing is enabled, the command also displays the weight of each queue.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 7.1	Command was expanded to include the **dscp-cos** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following is sample output from the **show qos cos-map** command for a NetVanta switch product:

```
>enable
#show qos cos-map
CoS Priority:    0   1   2   3   4   5   6   7
Priority Queue:  1   1   2   2   3   3   4   4
```

The following is sample output from the **show qos cos-map** command for a carrier Ethernet product:

```
>enable
#show qos cos-map
VLAN Priority:   0   1   2   3   4   5   6   7
Queue:           1   0   2   3   4   5   6   7
```

The following is sample output from the **show qos interface** command for Ethernet 0/8 interface:

```
>enable
#show qos interface ethernet 0/8
 Ethernet 0/8
 trust state: trusted
 default CoS: 0
```

The following is sample output from the **show qos queuing** command with WRR queuing enabled:

```
>enable
#show qos queuing
Queue-type: wrr
Expedite queue: disabled
wrr weights:
 qid - weight
 1 - 12
 2 - 45
 3 - 55
 4 - 65
```

show qos map

Use the **show qos map** command to display information about the quality of service (QoS) map. This information differs based on how a particular map entry is defined. Variations of this command include the following:

show qos map
show qos map <*name*>
show qos map <*name*> <*number*>
show qos map interface <*interface*>
show qos map interface <*interface*> **extended**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*name*>	Optional. Specifies the name of a defined QoS map.
<*number*>	Optional. Specifies one of the map's defined sequence numbers.
interface <*interface*>	Optional. Displays the QoS map information for a specific interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show qos map interface ?** command for a complete list of interfaces.
extended	Optional. Includes the broadcast, multicast, and unicast counts in the display output.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) interface.
Release 11.1	Demand interface was added.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release R11.1.0	Command was expanded to include the Ethernet in the first mile (EFM) group, system control Ethernet virtual connection (EVC) and the system management EVC.
Release R11.4.0	Output for **show qos map interface** command was changed to include packet match statistics.
Release R11.5.0	Command was expanded to include the **extended** parameter.
Release R11.9.0	Command was expanded to include the tunnel interface.
Release R13.11.0	Output for the **show qos map interface** command for Gigabit Ethernet subinterfaces was changed to include Layer 3 ingress and egress bytes for both the UNI and NNI on a per-subinterface per-queue basis. Ingress and egress bytes are displayed in the **Ingress Aggregate Bytes** and **Egress Aggregate Bytes** output lines of the command output.

Usage Examples

The following example shows all QoS maps and all entries in those maps:

```
>enable
#show qos map
qos map priority
  map entry 10
    match IP packets with a precedence value of 6
    priority bandwidth: 400 (kilobits/sec) burst: default
  map entry 20
    match ACL icmp
  map entry 30
    match RTP packets on even destination ports between 16000 and 17000
  map entry 50
    match ACL tcp
  map entry 60
  match IP packets with a dscp value of 2
  set dscp value to 6
  map entry 70
  match NetBEUI frames being bridged by the router
  priority bandwidth: 150 (kilobits/sec) burst: default
  qos map tcp_map
  map entry 10
    match ACL tcp
    priority bandwidth: 10 (kilobits/sec) burst: default
    set precedence value to 5
  map entry 20
    match IP packets with a precedence value of 3
    priority bandwidth: 50 (kilobits/sec) burst: default
```


The following example shows the QoS map named **priority** and all entries in that map:

```
>enable
#show qos map priority
  qos map priority
  map entry 10
   match IP packets with a precedence value of 6
   priority bandwidth: 400 (kilobits/sec) burst: default
  map entry 20
   match ACL icmp
  map entry 30
   match RTP packets on even destination ports between 16000 and 17000
  map entry 50
   match ACL tcp
  map entry 60
   match IP packets with a dscp value of 2
   set dscp value to 6
  map entry 70
   match NetBEUI frames being bridged by the router
   priority bandwidth: 150 (kilobits/sec) burst: default
```

The following example shows only QoS map named **priority** with the sequence number **10**:

```
>enable
#show qos map priority 10
  qos map priority
  map entry 10
   match IP packets with a precedence value of 6
   priority bandwidth: 400 (kilobits/sec) burst: default
```

The following examples show QoS map interface statistics associated with the applied map for the Frame Relay 1 interface:

```
>enable
#show qos map interface frame-relay 1
fr 1
qos-policy out: priority
  map entry 10
   match IP packets with a precedence value of 6
   budget 145/10000 bytes (current/max)
   priority bandwidth: 400 (kilobits/sec)
   packets matched on interface: 27289
   packets dropped: 0

  map entry 20
   match IP packets with a DSCP value of af41
   class bandwidth: 40 (% of remaining)
```



```
    conversation: 235
    packets matched: 23457
    packets dropped: 0

>enable
#show qos map int gig 0/2.1
 giga-eth 0/2.1
  qos-policy out: MAP_OUT
   map entry 11
     match ip dscp af11
     set egress-queue value to 0
     packets matched: 7, bytes matched: 1022
     5 minute offered rate 0 bits/sec
   map entry 12
     match ip dscp af12
     set egress-queue value to 0
     packets matched: 0, bytes matched: 0
     5 minute offered rate 0 bits/sec
   map entry 13
     match ip dscp af13
     set egress-queue value to 0
     packets matched: 5, bytes matched: 730
     5 minute offered rate 16 bits/sec
   map entry default
     packets matched: 26, bytes matched: 4812
     5 minute offered rate 72 bits/sec

 giga-eth 0/2.1
  qos-policy in: MAP_IN (enabled)
   map entry 11
     match ip dscp af11
     set DSCP value to 0
     packets matched: 7, bytes matched: 896
     5 minute offered rate 0 bits/sec, drop rate 0 bits/sec
   map entry 12
     match ip dscp af12
     set DSCP value to 0
     packets matched: 5, bytes matched: 640
     5 minute offered rate 16 bits/sec
   map entry 13
     match ip dscp af13
     set DSCP value to 0
     packets matched: 5, bytes matched: 640
     5 minute offered rate 16 bits/sec, drop rate 0 bits/sec
```



```
  map entry default
    packets matched: 0, bytes matched: 0
    5 minute offered rate 0 bits/sec
```


show queue *<interface>*

Use the **show queue** command to display conversation information associated with an interface queue. This command shows summary and per-conversation information. The per-conversation details are only displayed if the interface has sufficient traffic to be congested and packets are being held in the interface queue. Variations of this command include:

show queue *<interface>*
show queue *<interface>* **child**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Displays the queueing information for the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type the **show queue ?** command to display a list of valid interfaces.
child	Optional. Displays the subqueue statistics.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) interface.
Release 11.1	Demand interface was added.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.4	Command was expanded to include the **child** keyword.
Release 17.5	Command was expanded to include the asynchronous transfer mode (ATM) and Frame Relay interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.

Usage Examples

The following is sample output from the **show queue** command:

```
>enable
#show queue ethernet 0/2
 Queueing method: weighted fair
 Output queue: 4/222/540/64/176 (size/highest/max total/threshold/drops)
    Conversations 0/4/256 (active/max active/max total)
    Available Bandwidth 15000 kilobits/sec

   (depth/weight/matches/discards) 4/32768/32456/0
   Conversation 178, linktype: ip, length: 936
   source: 10.22.13.34, destination: 10.22.2.3, id: 0xddc6, ttl: 127,
   TOS: 0 prot: 6 (tcp), source port 1086, destination port 20
```

show queue interfaces

Use the **show queue interfaces** command to display the contents and queuing method for Layer 3 interface queues. Variations of this command include:

show queue interfaces efm-group
show queue interfaces efm-group <*slot/group*>
show queue interfaces efm-group <*slot/group*> **counters**
show queue interfaces efm-group <*slot/group*> **counters** <*queue*>
show queue interfaces efm-group <*slot/group*> **performance-statistics 15-minute**
show queue interfaces efm-group <*slot/group*> **performance-statistics 15-minute** <*value*>
show queue interfaces efm-group <*slot/group*> **performance-statistics 24-hour**
show queue interfaces efm-group <*slot/group*> **performance-statistics 24-hour** <*value*>
show queue interfaces efm-group <*slot/group*> <*queue*>
show queue interfaces efm-group <*slot/group*> <*queue*> **performance-statistics 15-minute**
show queue interfaces efm-group <*slot/group*> <*queue*> **performance-statistics 15-minute** <*value*>
show queue interfaces efm-group <*slot/group*> <*queue*> **performance-statistics 24-hour**
show queue interfaces efm-group <*slot/group*> <*queue*> **performance-statistics 24-hour** <*value*>
show queue interfaces gigabit-ethernet
show queue interfaces gigabit-ethernet <*slot/port*>
show queue interfaces gigabit-ethernet <*slot/port*> **counters**
show queue interfaces gigabit-ethernet <*slot/port*> **counters** <*queue*>
show queue interfaces gigabit-ethernet <*slot/port*> **counters nni**
show queue interfaces gigabit-ethernet <*slot/port*> **performance-statistics 15-minute**
show queue interfaces gigabit-ethernet <*slot/port*> **performance-statistics 15-minute** <*value*>
show queue interfaces gigabit-ethernet <*slot/port*> **performance-statistics 24-hour**
show queue interfaces gigabit-ethernet <*slot/port*> **performance-statistics 24-hour** <*value*>
show queue interfaces gigabit-ethernet <*slot/port*> <*queue*>
show queue interfaces gigabit-ethernet <*slot/port*> <*queue*> **performance-statistics 15-minute**
show queue interfaces gigabit-ethernet <*slot/port*> <*queue*> **performance-statistics 15-minute** <*value*>
show queue interfaces gigabit-ethernet <*slot/port*> <*queue*> **performance-statistics 24-hour**
show queue interfaces gigabit-ethernet <*slot/port*> <*queue*> **performance-statistics 24-hour** <*value*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

efm-group <*slot/group*>	Displays queue information for a specific EFM group. Valid EFM group range is **1** to **1024**. If the slot and group are not specified, queue information for all EFM groups is displayed.

gigabit-ethernet <*slot/port*>	Displays queue information for the Gigabit Ethernet interface. If the slot and port are not specified, queue information for all Gigabit Ethernet interfaces is displayed.
counters	Optional. Displays Metro Ethernet Forum (MEF) user network interface (UNI) counters for the specified interface. If <*queue*> is specified, displays only the counters for the specified queue on the specified interface.
<*queue*>	Optional. Limits the output of this command to a single queue associated with the interface. Valid range is **0** to **7**.
nni	Optional. Displays Metro Ethernet Forum (MEF) network-to-network interface (NNI) counters for the specified interface.
performance-statistics	Optional. Displays aggregate performance statistics.
15-minute	Optional. Displays the statistics for a 15-minute period in the last 24 hours.
24-hour	Optional. Displays the statistics for a 24-hour period in the last 7 days.
<*value*>	Optional. Specifies which 15-minute period in the last 24 hours or which 24-hour period in the last 7 days is displayed. Range for 15-minute periods is **1** to **96**; range for 24-hour periods is **1** to **7**.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.
Release R11.5.0	Command was expanded to include **counters** and **performance-statistics** parameters.
Release R13.11.0	Command was expanded to include the **nni** parameter. In addition, command output was changed to include ingress and egress Layer 2 bytes.

Usage Examples

The following example displays queue information for the Gigabit Ethernet interface 1/1:

```
>enable
#show queue interfaces gigabit-ethernet 1/1
Queuing method: fifo
Output queue: 0/256/0 (size/max total/drops)
```


show queue priority max-configured

Use the **show queue priority max-configured** command to display the configured maximum number of priority queues for quality of service (QoS) maps. Priority queues are configured using the command *priority queue-limit <value> on page 4485*.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.3.0	Command was introduced.

Usage Examples

The following example displays the QoS map priority queue limit:

```
>enable
#show queue priority max-configured
Total maximum configured priority queue-limit: 256
```

show queuing

Use the **show queuing** command to display information associated with configured queuing methods. Variations of this command include:

show queuing
show queuing fair

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

fair	Optional. Displays only information on the weighted fair queuing (WFQ) configuration.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show queuing** command:

```
>enable
#show queuing
  Interface        Discard threshold    Conversation subqueues
  fr 1             64                   256
  fr 2             64                   256
  ppp 1            64                   256
```


show radius statistics

Use the **show radius statistics** command to display various statistics from the remote authentication dial-in user service (RADIUS) subsystem. These statistics include number of packets sent, number of invalid responses, number of timeouts, average packet delay, and maximum packet delay. Statistics are shown for both authentication and accounting packets.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show radius statistics** command:

```
>enable
#show radius statistics
                              Auth.       Acct.
Number of packets sent:       3           0
Number of invalid responses:  0           0
Number of timeouts:           0           0
Average delay:                2 ms        0 ms
Maximum delay:                3 ms        0 ms
```

show ramdisk

Use the **show ramdisk** command to display a list of all files currently stored in volatile random access memory (RAM) disk memory or details about a specific file stored in RAM disk memory. Variations of this command include:

show ramdisk
show ramdisk *<filename>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

> *Not all units are capable of using a RAM disk file system. Use the **show ?** command to display a list of valid commands at the enable prompt.*

Syntax Description

<filename>	Optional. Displays details for a specified file located in RAM disk file system. Enter a wildcard (such as ***.biz**) to display the details for all files matching the entered pattern.

Default Values

No default values are necessary for this command.

Command History

Release 17.7	Command was introduced for AOS units limited to only 16 Megabytes of flash memory.

Usage Examples

The following is sample **show ramdisk** output displaying the contents of the RAM disk, space occupied by each file, the total RAM disk space allocated, available space, and used space:

```
>enable
#show ramdisk
10005125 NV3130A-17-07-00-26-AE.biz
10007923 bytes used, 7429514 available, 17437437 total
```


show route-map

Use the **show route-map** command to display any route maps that have been configured in the router. This command displays any match and set clauses associated with the route map, as well as the number of incoming routes that have matched each route map. Route maps can be used for Border Gateway Protocol (BGP) and PBR. Variations of this command include:

show route-map
show route-map *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Optional. Displays only the route map matching the specified name.

Default Values

By default, this command displays all defined route maps.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

In the example below, all route maps in the router are displayed.

```
>enable
#show route-map
route-map RouteMap1, permit, sequence 10
 Match clauses:
   community (community-list filter): CommList1
 Set clauses:
   local-preference 250
 BGP Filtering matches: 75 routes
 Policy routing matches: 0 packets 0 bytes
route-map RouteMap1, permit, sequence 20
 Match clauses:
   community (community-list filter): CommList2
```



```
 Set clauses:
   local-preference 350
 BGP Filtering matches: 87 routes
 Policy routing matches: 0 packets 0 bytes
route-map RouteMap2, permit, sequence 10
 Match clauses:
   ip address (access-lists): Acl1
 Set clauses:
   metric 100
 BGP Filtering matches: 10 routes
 Policy routing matches: 0 packets 0 bytes
route-map RouteMap2, permit, sequence 20
 Match clauses:
   ip address (access-lists): Acl2
 Set clauses:
   metric 200
 BGP Filtering matches: 12 routes
 Policy routing matches: 0 packets 0 bytes
route-map RouteMap3, permit, sequence 10
 Match clauses:
   length 150 200
 Set clauses:
   ip next-hop: 10.10.11.254
 BGP Filtering matches: 0 routes
 Policy routing matches: 0 packets 0 bytes
route-map RouteMap3, permit, sequence 20
 Match clauses:
   ip address (access-lists): Acl3
 Set clauses:
   ip next-hop: 10.10.11.14
 BGP Filtering matches: 0 routes
 Policy routing matches: 144 packets 15190 bytes
```

In the example below, only **RouteMap2** is displayed.

```
>enable
#show route-map RouteMap2
route-map RouteMap2, permit, sequence 10
 Match clauses:
   ip address (access-lists): Acl1
 Set clauses:
   metric 100
 BGP Filtering matches: 10 routes
 Policy routing matches: 0 packets 0 bytes
route-map RouteMap2, permit, sequence 20
--MORE--
```


show rps

Use the **show rps** command to show information related to the redundant power supply (RPS) power state. The output of this command indicates if an RPS is connected, if it is delivering power, the available power, and whether the RPS has failed.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.8.0	Command was introduced.

Usage Examples

The following is sample output from this command:

```
>enable
#show rps
VCID 1 RPS is connected
VCID 1 RPS is not delivering power
VCID 2 RPS is connected
VCID 2 RPS is not delivering power
```


show rtp media sessions

Use the **show rtp media sessions** command to display all of the anchored Realtime Transport Protocol (RTP) flow associations and the number of relayed packets per association currently active in an anchored RTP flow. In addition, the time to live (TTL) and the session type (digital signal processor (DSP), media anchored, or transcoded) for the association is displayed.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.4.0	Command was introduced and replaced the **show ip rtp media-anchoring sessions** command.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example displays a summary of all gathered media statistics:

```
>enable
#show rtp media sessions
  CallID  Anchored Address      Remote Address       TTL   Pkts     Ovrd  Type   Sess
  ------------------------------------------------------------------------------------------------------------------------
   7      10.10.10.1:40008      10.10.10.2:2230      45    108062   No    Audio  Xcode
   7      10.17.250.12:40010    10.17.250.14:10262   45    108063   No    Audio  Xcode
   7      10.10.10.1:40009      10.10.10.2:2231      44    432      No    Audio  Xcode
   7      10.17.250.12:40011    10.17.250.14:10263   44    432      No    Audio  Xcode
```


show rtp quality-monitoring

Use the **show rtp quality-monitoring** command to display a summary of all voice quality monitoring (VQM) statistics gathered from monitoring inbound Realtime Transport Protocol (RTP) streams across the network.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example displays a summary of all gathered VQM statistics:

#show rtp quality-monitoring

```
Voice Quality Monitoring is ENABLED
Jitter Buffer: adaptive 10/50/100 ms (min/nominal/max)

Quality     Active Streams      Call History    All Streams     MOS range
----------  ------------------  --------------  --------------  ----------------
Excellent   60                  50              13462           4.40 - 4.00
Good        20                  37              3456            3.99 - 3.60
Fair        3                   1               45              3.59 - 2.60
Poor        1                   7               7               2.59 - 0.00
----------  ------------------  --------------  --------------  ----------------
Totals:     84                  95              16970

(Note: Statistics for All Streams are updated at call completion and do not include currently active
streams. Call history statistics are available for up to 100 streams.)

History thresholds:
MOS (LQ/CQ/PQ): 3.0/3.0/3.0
```


Loss: 20 pkts
Out-of-order packets: 300 pkts
Jitter: 300 ms

Notification thresholds:

Metric	Info	Notice	Warning	Error
PQ MOS	4.4	4.0	3.6	2.6
LQ MOS	4.4	4.0	3.6	2.6
Loss	N/A	25	50	100 pkts
Out-of-order	N/A	N/A	50	100 pkts
Jitter	N/A	20	100	300 ms

Traps: ENABLED at Notice

Traps sent: 14

show rtp quality-monitoring active-calls

Use the **show rtp quality-monitoring active-calls** command to display the voice quality monitoring (VQM) statistics gathered from monitoring active calls on inbound Realtime Transport Protocol (RTP) streams across the network. These statistics can be sorted by mean opinion score (MOS), jitter, or lost or out-of-order packets. Variations of this command include:

show rtp quality-monitoring active-calls
show rtp quality-monitoring active-calls call-id <*string*>
show rtp quality-monitoring active-calls degradation
show rtp quality-monitoring active-calls detail
show rtp quality-monitoring active-calls from-uri <*string*>
show rtp quality-monitoring active-calls sort-by jitter
show rtp quality-monitoring active-calls sort-by loss
show rtp quality-monitoring active-calls sort-by lq-mos
show rtp quality-monitoring active-calls sort-by out-of-order
show rtp quality-monitoring active-calls sort-by pq-mos
show rtp quality-monitoring active-calls source-uri <*string*>
show rtp quality-monitoring active-calls to-uri <*string*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

call-id <*string*>	Optional. Displays active call statistics based on a substring of the Call-ID.
degradation	Optional. Displays possible sources of voice quality degradation for active calls.
detail	Optional. Displays details of all available active call statistics.
from-uri <*string*>	Optional. Displays active call statistics based on a substring of the From URI.
sort-by jitter	Optional. Displays active call statistics with the highest amount of jitter first.
sort-by loss	Optional. Displays active call statistics with the highest number of lost packets first.
sort-by lq-mos	Optional. Displays active call statistics with the lowest listening quality (LQ) MOS first.
sort-by out-of-order	Optional. Displays active call statistics with the highest number of out-of-order packets first.
sort-by pq-mos	Optional. Displays active call statistics with the lowest perceived quality (PQ) MOS first.

source-uri <*string*>	Optional. Displays active call statistics based on a substring of the URI/extension from which the RTP stream is sourced.
to-uri <*string*>	Optional. Displays active call statistics based on a substring of the To uniform resource identifier (URI) or extension to which this RTP stream is destined.

Default Values

By default, only the most commonly used statistics are shown.

Functional Notes

These statistics will not be available if VQM is disabled.

Command History

Release 17.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

In the following example, VQM active call statistics are sorted by lost packets:

```
#show rtp quality-monitoring active-calls sort-by loss
    Displaying 30 estimated stream statistics from 15 completed calls

    RTP stream: 3.3.3.3 : 50000, ppp 1 -> 1.1.1.1 : 3000, vlan 1
    To: 5551234@voip.com
        Call-start (duration): 11 Apr 2010 20:58:39 (93 s)
        MOS LQ: 3.800
        MOS PQ: 3.800
        Loss: 413 pkts
        Out-of-order: 30 pkts
        Jitter (max): 20 ms
        CODEC: g711

    RTP stream: 1.1.1.1 : 3000, vlan 1 -> 3.3.3.3: 50000, ppp 1
    To: 5551234@voip.com
    From: 5551235@voip.com
        Call-start (duration): 11 Apr 2010 20:58:39 (93 s)
        MOS LQ: 3.800
        MOS PQ: 3.800
        Loss: 0 pkts
        Out-of-order: 0 pkts
        Jitter (max): 1 ms
        CODEC: g711
--MORE--
```


show rtp quality-monitoring call-history

Use the **show rtp quality-monitoring call-history** command to display the voice quality monitoring (VQM) statistics gathered from previously monitored calls on inbound Realtime Transport Protocol (RTP) streams. These calls are stored in the VQM call history. These statistics can be sorted by mean opinion score (MOS), jitter, or lost or out-of-order packets. Variations of this command include:

show rtp quality-monitoring call-history
show rtp quality-monitoring call-history call-id <*string*>
show rtp quality-monitoring call-history degradation
show rtp quality-monitoring call-history detail
show rtp quality-monitoring call-history from-uri <*string*>
show rtp quality-monitoring call-history sort-by jitter
show rtp quality-monitoring call-history sort-by loss
show rtp quality-monitoring call-history sort-by lq-mos
show rtp quality-monitoring call-history sort-by out-of-order
show rtp quality-monitoring call-history sort-by pq-mos
show rtp quality-monitoring call-history source-uri <*string*>
show rtp quality-monitoring call-history to-uri <*string*>
show rtp quality-monitoring call-history degradation
show rtp quality-monitoring call-history detail

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

call-id <*string*>	Optional. Displays past call statistics based on a substring of the Call-ID.
degradation	Optional. Displays possible sources of voice quality degradation for past calls.
detail	Optional. Displays details of all available past call statistics.
from-uri <*string*>	Optional. Displays past call statistics based on a substring of the From URI.
sort-by jitter	Optional. Displays past call statistics with the highest amount of jitter first.
sort-by loss	Optional. Displays past call statistics with the highest number of lost packets first.
sort-by lq-mos	Optional. Displays past call statistics with the lowest listening quality (LQ) MOS first.
sort-by out-of-order	Optional. Displays past call statistics with the highest number of out-of-order packets first.

sort-by pq-mos	Optional. Displays past call statistics with the lowest perceived quality (PQ) MOS first.
source-uri <*string*>	Optional. Displays past call statistics based on a substring of the URI/extension from which the RTP stream is sourced.
to-uri <*string*>	Optional. Displays past call statistics based on a substring of the To uniform resource identifier (URI) or extension to which this RTP stream is destined.

Default Values

By default, only the most commonly used statistics are shown.

Functional Notes

These statistics will still be available even if VQM is disabled.

Command History

Release 17.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

In the following example, VQM past call statistics are sorted by lost packets:

```
#show rtp quality-monitoring call-history sort-by loss
    Displaying 30 estimated stream statistics from 15 completed calls

    RTP stream: 3.3.3.3 : 50000, ppp 1 -> 1.1.1.1 : 3000, vlan 1
    To: 5551234@voip.com
        Call-start (duration): 11 Apr 2010 20:58:39 (93 s)
        MOS LQ: 3.800
        MOS PQ: 3.800
        Loss: 413 pkts
        Out-of-order: 30 pkts
        CODEC: g711

    RTP stream: 1.1.1.1 : 3000, vlan 1 -> 3.3.3.3: 50000, ppp 1
    To: 5551234@voip.com
    From: 5551235@voip.com
        Call-start (duration): 11 Apr 2010 20:58:39 (93 s)
        MOS LQ: 3.800
        MOS PQ: 3.800
        Loss: 0 pkts
        Out-of-order: 0 pkts
        CODEC: g711
--MORE--
```


show rtp quality-monitoring endpoints

Use the **show rtp quality-monitoring endpoints** command to display the voice quality monitoring (VQM) statistics gathered on inbound Realtime Transport Protocol (RTP) streams for all voice endpoints. These statistics can be sorted by mean opinion score (MOS), jitter, or lost or out-of-order packets. Variations of this command include:

show rtp quality-monitoring endpoints
show rtp quality-monitoring endpoints sort-by jitter
show rtp quality-monitoring endpoints sort-by loss
show rtp quality-monitoring endpoints sort-by lq-mos
show rtp quality-monitoring endpoints sort-by out-of-order
show rtp quality-monitoring endpoints sort-by pq-mos
show rtp quality-monitoring endpoints summary

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

sort-by jitter	Optional. Displays voice endpoint statistics with the highest amount of jitter first.
sort-by loss	Optional. Displays voice endpoint statistics with the highest number of lost packets first.
sort-by lq-mos	Optional. Displays voice endpoint statistics with the lowest listening quality (LQ) MOS first.
sort-by out-of-order	Optional. Displays voice endpoint statistics with the highest number of out-of-order packets first.
sort-by pq-mos	Optional. Displays voice endpoint statistics with the lowest perceived quality (PQ) MOS first.
summary	Optional. Displays a summary of all voice endpoint VQM statistics.

Default Values

By default, only the most commonly used statistics are shown.

Functional Notes

These statistics will still be available even if VQM is disabled.

Command History

Release 17.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

In the following example, VQM endpoint statistics are summarized:

#show rtp quality-monitoring endpoints summary

Displaying 2 estimated endpoint statistics from 50 completed calls

RTP source: 3.3.3.3, ppp 1

Quality	Completed Calls	MOS range
Excellent	0	4.40 - 4.00
Good	0	3.99 - 3.60
Fair	24	3.59 - 2.60
Poor	3	2.59 - 0.00
Totals:	27 (of the last 100 recorded calls)	

RTP source: 5.5.5.5, ppp 1

show rtp quality-monitoring interface

Use the **show rtp quality-monitoring interface** command to display the voice quality monitoring (VQM) statistics gathered from monitored calls on inbound Realtime Transport Protocol (RTP) streams across interfaces with VQM enabled. These statistics can be sorted by mean opinion score (MOS), jitter, or lost or out-of-order packets. Variations of this command include:

show rtp quality-monitoring interface
show rtp quality-monitoring interface *<interface>*
show rtp quality-monitoring interface *<interface>* **detail**
show rtp quality-monitoring interface detail
show rtp quality-monitoring interface *<interface>* **sort-by jitter**
show rtp quality-monitoring interface sort-by jitter
show rtp quality-monitoring interface *<interface>* **sort-by loss**
show rtp quality-monitoring interface sort-by loss
show rtp quality-monitoring interface *<interface>* **sort-by lq-mos**
show rtp quality-monitoring interface sort-by lq-mos
show rtp quality-monitoring interface *<interface>* **sort-by out-of-order**
show rtp quality-monitoring interface sort-by out-of-order
show rtp quality-monitoring interface *<interface>* **sort-by pq-mos**
show rtp quality-monitoring interface sort-by pq-mos
show rtp quality-monitoring interface *<interface>* **summary**
show rtp quality-monitoring interface summary

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Optional. Displays details of all available VQM interface statistics.
<interface>	Optional. Displays VQM statistics for a specific interface. Specify the interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**.
sort-by jitter	Optional. Displays VQM interface statistics with the highest amount of jitter first.
sort-by loss	Optional. Displays VQM interface statistics with the highest number of lost packets first.
sort-by lq-mos	Optional. Displays VQM interface statistics with the lowest listening quality (LQ) MOS first.

sort-by out-of-order	Optional. Displays VQM interface statistics with the highest number of out-of-order packets first.
sort-by pq-mos	Optional. Displays VQM interface statistics with the lowest perceived quality (PQ) MOS first.
summary	Optional. Displays a summary of VQM interface statistics.

Default Values

By default, only the most commonly used statistics are shown.

Functional Notes

These statistics will still be available even if VQM is disabled.

Command History

Release 17.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

In the following example, a summary of all VQM interface statistics is shown:

```
#show rtp quality-monitoring interface summary
    ppp 1
        Quality         Completed Calls         MOS range
        -----------     ------------------------ -----------------
        Excellent       0                       4.40 - 4.00
        Good            2                       3.99 - 3.60
        Fair            34                      3.59 - 2.60
        Poor            3                       2.59 - 0.00
        -----------     ------------------------ -----------------
        Totals:         37 (of the last 100 recorded calls)

    vlan 1
        Quality         Completed Calls         MOS range
        -----------     ------------------------ -----------------
        Excellent       36                      4.40 - 4.00
        Good            1                       3.99 - 3.60
        Fair            0                       3.59 - 2.60
        Poor            0                       2.59 - 0.00
        -----------     ------------------------ -----------------
        Totals:         37 (of the last 100 recorded calls)
```


show rtp quality-monitoring reporter

Use the **show rtp quality-monitoring reporter** command to display voice quality monitoring (VQM) reporter statistics. Variations of this command include:

show rtp quality-monitoring reporter
show rtp quality-monitoring reporter realtime
show rtp quality-monitoring reporter <*name*>
show rtp quality-monitoring reporter <*name*> **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<*name*>	Optional. Specifies that only the statistics for the named VQM reporter are displayed.
realtime	Optional. Specifies that output is displayed in real time.

Default Values

No default values are necessary for this command.

Command History

Release 17.6	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

Output of the **show rtp quality-monitoring reporter** command displays the reporter name (**Name**), the queue volume or how many reports are waiting to send requests or receive responses (**Depth**), how many successful responses have been received (**Success**), how many failure responses have been received (**Failed**), how many requests have been transmitted (**Request**), how many challenge responses have been received (**Chalnge**), how many requests did not receive responses at all (**Rollovr**), and how many reports were discarded because the retry limit was exceeded (**Discard**).

Usage Examples

The following is sample output from this command showing VQM reporter statistics for all configured VQM reporters:

>**enable**
#show rtp quality-monitoring reporter

Name	Depth	Success	Failed	Request	Chalnge	Rollovr	Discard
Test 1	4	0	0	36	0	36	6
Test 2	4	0	0	36	0	36	6
Test 3	0	0	10	10	0	0	0
Test 4	0	0	10	10	0	0	0
Test 5	0	0	0	0	0	0	0

show rtp resources

Use the **show rtp resources** command to display Realtime Transfer Protocol (RTP) resource information. Variations of this command include:

show rtp resources
show rtp resources debug

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

debug	Optional. Activates the RTP resources event debug messages.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 14.1	Command was expanded to include more options.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show rtp resources** command:

```
>enable
#show rtp resources
DSP      Channel    Type     Port     Status
-------------------------------------------------------------------------
 0/1       1         RTP      N/A      Available
 0/1       2         RTP      N/A      Available
 0/1       3         RTP      N/A      Available
 0/1       4         RTP      N/A      Available
 0/1       5         RTP      N/A      Available
 0/1       6         RTP      N/A      Available
 0/1       7         RTP      N/A      Available
 0/1       8         RTP      N/A      Available
--MORE--
```


checksum	Optional. Displays the encrypted message digest 5 (MD5) version of the running configuration.
counter-profile	Optional. Displays the current running configuration for all counter profiles.
counter-profile <*slot/index*>	Optional. Displays the current running configuration for the specified counter profile. Specify a counter profile in the format <*slot/index*>. For example, **0/1**.
dynamic-counter	Optional. Displays the current running configuration for all counter profiles.
dynamic-counter <*slot/index*>	Optional. Displays the current running configuration for the specified counter profile. Specify a counter profile in the format <*slot/index*>. For example, **0/1**.
evc	Optional. Displays the current running configuration for all EVCs.
evc <*name*>	Optional. Displays the current running configuration for the specified EVC.
evc-map	Optional. Displays the current running configuration for all EVC maps.
evc-map <*name*>	Optional. Displays the current running configuration for the specified EVC map.
ethernet loopback facility	Optional. Displays the current running configuration for all facility loopback objects.
ethernet loopback terminal	Optional. Displays the current running configuration for all terminal loopback objects.
<*name*> <*slot*>	Optional. Displays the current running configuration for the facility or terminal loopback object with the specified name and slot identifier.
slot <*slot*>	Optional. Displays the current running configuration for all facility or terminal loopback objects with the specified slot identifier.
hmr	Optional. Displays the current running configuration for Session Initiation Protocol (SIP) header manipulation rules (HMR).
hmr policy	Optional. Displays the configured SIP HMR policies in the running configuration.
hmr policy <*name*>	Optional. Displays the specified SIP HMR policy in the running configuration.
hmr rule-set	Optional. Displays the configured SIP HMR rule sets in the running configuration.
hmr rule-set <*name*>	Optional. Displays the specified SIP HMR rule set in the running configuration.
ip access-lists	Optional. Displays the current running configuration for all configured IPv4 access control lists (ACLs).

interface <*interface*>	Optional. Displays the current running configuration for a particular interface. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show running-config interface ?** for a complete list of valid interfaces.
ip-crypto	Optional. Displays the current running configuration for all IPv4 Internet Protocol security (IPsec) virtual private network (VPN) settings.
ip mgcp	Optional. Displays the current running configuration for all Media Gateway Control Protocol (MGCP) parameters.
ip nat pool	Optional. Displays the current running configuration for IPv4 network address translation (NAT) pool parameters.
ip policy-class	Optional. Displays the current running configuration for all configured IPv4 access control policies (ACPs).
ip rtp	Optional. Displays the current running configuration for all IPv4 Realtime Transport Protocol (RTP) parameters.
ip security monitor	Optional. Displays the current running configuration for all IPv4 security monitor parameters.
ip urlfilter	Optional. Displays the current running configuration for all IPv4 uniform resource locator (URL) filters.
license	Optional. Displays the current running configuration for all software licenses.
license key	Optional. Displays the current running configuration for all software license keys.
mef	Optional. Displays the current running configuration for all Metro Ethernet Forum (MEF) components.
network-sync	Optional. Displays the current running configuration for network synchronization (Network Sync).
packet-capture	Optional. Displays the current running configuration for all configured packet captures.
<*name*>	Optional. Limits output to a single packet capture.
policer	Optional. Displays the current running configuration for all policers.
policer <*name*>	Optional. Displays the current running configuration for the specified policer.
probe	Optional. Displays the current configuration for all running probes.
qos-map	Optional. Displays the current running configuration for all configured quality of service (QoS) maps.

quality-monitoring	Optional. Displays the current running configuration for voice quality monitoring (VQM).
queue	Optional. Displays the current running configuration for all queues.
queue interface <*interface*>	Optional. Displays the current running configuration for all queues on the specified interface. Specify an interface in the format <*interface type [slot/group* | *slot/port* | *interface id*>. For example, for an EFM group interface, use **efm-group 1/3**; or for a Gigabit Ethernet interface, use **gigabit-ethernet 0/1**. Type **show running-config queue interface ?** for a complete list of valid interfaces.
router bgp	Optional. Displays the current Border Gateway Protocol (BGP) configuration.
router ospf	Optional. Displays the Open Shortest Path First version 2 (OSPFv2) configuration.
router ospfv3	Optional. Displays the OSPF version 3 (OSPFv3) configuration.
<*process id*>	Optional. Limits output to a single OSPFv3 process. Valid range is **1** to **65535**.
router pim-sparse	Optional. Displays the current global protocol-independent multicast-sparse mode (PIM-SM) configuration.
router rip	Optional. Displays the Routing Information Protocol (RIP) configuration.
sdp	Optional. Displays the current running configuration for all Session Description Protocol (SDP) parameters.
shaper	Optional. Displays the current running configuration for all traffic shapers.
shaper <*name*>	Optional. Displays the current running configuration for the specified traffic shaper.
sip	Optional. Displays the current running configuration for all Session Initiation Protocol (SIP) parameters.
sip proxy failover	Optional. Displays the current running configurations for SIP proxy failover.
sip proxy user-template <*name*>	Optional. Displays the current running configuration for the specified SIP proxy user template.
srtp-profile	Optional. Displays the current running configuration for any configured Secure Realtime Transfer Protocol (SRTP) profiles.
system-control-evc	Optional. Displays the current running configuration for the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Displays the current running configuration for the system management EVC.
tcl script <*name*>	Optional. Displays the specified tool command language (Tcl) script.

tls-profile	Optional. Displays the current running configuration for any configured Transport Layer Security (TLS) profiles.
track	Optional. Displays the current running configuration for all tracks.
vcid <*vcid*>	Optional. Displays the current running configuration for the specified virtual chassis ID of an ActivChassis member. Valid VCID range is **1** to **8**. VCID values **1** and **2** are given to the ActivChassis master and backup devices, respectively.
verbose	Optional. Displays the entire running configuration to the terminal screen (versus only the nondefault values).

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release 11.1	Demand, foreign exchange office (FXO), and serial interfaces were added. The **ip-crypto** and **router pim-sparse** keywords were added.
Release 13.1	Command was expanded to include the **ip rtp**, **ip sdp**, **probe** and **track** subcommands.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**, and the **ip urlfilter** and **quality-monitoring** keywords.
Release A1	Command was introduced in the AOS voice products.
Release A2	Command was expanded to include the **mgcp** parameter.
Release 17.4	Command was expanded to include the **ip nat pool** parameter.
Release 17.5	Command was expanded to include the **security monitor** parameter.
Release A4.01	Command was expanded to include the Ethernet in the first mile (EFM) group interface and the **ip sip proxy user-template** parameter. Command was expanded to include the Metro Ethernet Forum (MEF) parameter and the MEF Ethernet interface.
Release 17.9	Command was changed to require the **ip** keyword for the **access-list** and **policy-class** parameters for Adtran internetworking products only.
Release A4.05	Command was expanded to include the asymmetric digital subscriber line (ADSL) interface.
Release 18.2	Command was expanded to include the **ip sip proxy failover** parameter.

Release A5.01	Command was expanded to include the Gigabit Ethernet and gigabit switchport interfaces.
Release R10.1.0	Command was expanded to include the **hmr** parameters. Command was also changed to require the **ip** keyword for the **access-list** and **policy-class** parameters for Adtran voice products.
Release R10.4.0	Command was expanded to include the **license** and **license key** parameters.
Release R10.5.0	Command was expanded to include the **auto-config, router ospf**, **router ospfv3**, and **router rip** parameters.
Release R10.7.0	Command was expanded to include the **auto-link**, **packet-capture**, and **vcid** parameters.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword from the **sdp** and **sip** parameters.
Release R10.11.0	Command was expanded to include the **counter-profile**, **dynamic-counter**, and **network-sync** parameters.
Release R11.1.0	Command was expanded to include the very high-speed digital subscriber line (VDSL) interfaces and the **ethernet loopback facility** and **tcl script** parameter.
Release R11.3.0	Command was expanded to include the <*process id*> parameter for OSPFv2.
Release R11.5.0	Command was expanded to include the **evc**, **evc-map**, **policer**, **queue**, **queue interface efm-group, queue interface gigabit-ethernet, shaper**, **srtp profile**, **system-control-evc**, **system-management-evc**, and **tls profile** parameters.
Release R11.7.0	Command was expanded to include the 10 Gigabit switchport interface.
Release R13.7.0	Command was expanded to include the **terminal** loopback parameter.

Usage Examples

The following is sample output from the **show running-config** command:

```
>enable
#show running-config
Building configuration...
!
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
```



```
logging forwarding priority-level info
no logging email
!
!ip policy-timeout tcp all-ports 600
ip policy-timeout udp all-ports 60
ip policy-timeout icmp 60
!
interface eth 0/1
--MORE--
```

show running-config ipv6

Use the **show running-config ipv6** command to display all the nondefault parameters contained in the current Internet Protocol version 6 (IPv6) running configuration file. Specific portions of the running configuration may be displayed, based on the command entered. Variations of this command include the following:

show running-config ipv6 access-lists
show running-config ipv6 access-lists verbose
show running-config ipv6 crypto
show running-config ipv6 crypto verbose
show running-config ipv6 dhcp pool <*name*>
show running-config ipv6 dhcp pool <*name*> **verbose**
show running-config ipv6 policy-class
show running-config ipv6 policy-class verbose

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

access-lists	Displays the current running configuration for all configured IPv6 access control lists (ACLs).
crypto	Displays the current running configuration for all configured IPv6 crypto functions.
dhcp pool <*name*>	Displays the current running configuration for the specified Dynamic Host Control Protocol version 6 (DHCPv6) server address pool.
policy-class	Displays the current running configuration for all configured IPv6 access control policies (ACPs).
verbose	Optional. Displays the entire running configuration to the terminal screen (versus only the nondefault values).

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release 18.3	Command was expanded to include the **dhcp pool** parameter.
Release R10.7.0	Command was expanded to include the **crypto** parameter.

Usage Examples

The following example displays the IPv6 ACLs in the unit's running configuration:

```
>enable
#show running-config ipv6 access-lists
    ipv6 access-list extended Privatev6
        deny tcp any eq telnet any
        deny tcp any any eq telnet
        permit ipv6 any host 2000:1::1
        permit icmp any any
```

The following example displays the configured IPv6 ACPs in the unit's running configuration:

```
>enable
#show running-config ipv6 policy-class
ipv6 policy-class UNTRUSTED
        allow list localservicev6
        discard list Webtraffic
```

show running-config voice

Use the **show running-config voice** command to show running voice configurations. Variations of this command include the following:

show running-config voice
show running-config voice ani
show running-config voice ani verbose
show running-config voice ani-list
show running-config voice ani-list verbose
show running-config voice ani-list <*name*>
show running-config voice ani-list <*name*> **verbose**
show running-config voice autoattendant
show running-config voice autoattendant verbose
show running-config voice class-of-service
show running-config voice class-of-service verbose
show running-config voice class-of-service <*name*>
show running-config voice class-of-service <*name*> **verbose**
show running-config voice directory
show running-config voice directory verbose
show running-config voice grouped-trunk
show running-config voice grouped-trunk verbose
show running-config voice grouped-trunk <*name*>
show running-config voice grouped-trunk <*name*> **verbose**
show running-config voice line
show running-config voice line verbose
show running-config voice line <*number*>
show running-config voice line <*number*> **verbose**
show running-config voice mail
show running-config voice mail verbose
show running-config voice match
show running-config voice match ani
show running-config voice match ani verbose
show running-config voice mgcp-endpoint
show running-config voice mgcp-endpoint verbose
show running-config voice mgcp-endpoint <*index*>
show running-config voice mgcp-endpoint <*index*> **verbose**
show running-config voice music-on-hold
show running-config voice music-on-hold mode
show running-config voice music-on-hold player
show running-config voice music-on-hold player <*name*>
show running-config voice music-on-hold preferredCodec
show running-config voice named-digit-timeouts
show running-config voice named-digit-timeouts verbose
show running-config voice named-digit-timeouts <*name*>
show running-config voice named-digit-timeouts <*name*> **verbose**

show running-config voice operator-group
show running-config voice operator-group verbose
show running-config voice paging-group
show running-config voice paging-group verbose
show running-config voice paging-group *<extension>*
show running-config voice paging-group *<extension>* **verbose**
show running-config voice pickup-group
show running-config voice pickup-group *<name>*
show running-config voice queue
show running-config voice queue *<extension>*
show running-config voice queue verbose
show running-config voice queue *<extension>* **verbose**
show running-config voice ring-group
show running-config voice ring-group verbose
show running-config voice ring-group *<name>*
show running-config voice ring-group *<name>* **verbose**
show running-config voice ring-option
show running-config voice ring-option verbose
show running-config voice ring-option *<name>*
show running-config voice ring-option *<name>* **verbose**
show running-config voice speed-dial
show running-config voice speed-dial verbose
show running-config voice spre
show running-config voice spre verbose
show running-config voice spre-map
show running-config voice spre-map verbose
show running-config voice status-group
show running-config voice status-group verbose
show running-config voice status-group *<name>*
show running-config voice status-group *<name>* **verbose**
show running-config voice trunk
show running-config voice trunk verbose
show running-config voice trunk *<Txx>*
show running-config voice trunk *<Txx>* **verbose**
show running-config voice trunk-list
show running-config voice trunk-list verbose
show running-config voice trunk-list *<name>*
show running-config voice trunk-list *<name>* **verbose**
show running-config voice user
show running-config voice user verbose
show running-config voice user *<number>*
show running-config voice user *<number>* **verbose**
show running-config voice user *<name>*
show running-config voice user *<name>* **verbose**
show running-config voice user *<name>* *<last name>*
show running-config voice user *<name>* *<last name>* **verbose**

show running-config voice verbose

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

ani	Optional. Displays automatic number identification (ANI) substitution configurations.
ani-list	Optional. Displays all ANI list configurations.
ani-list <*name*>	Optional. Deploys a specific ANI list configuration.
autoattendant	Optional. Displays auto attendant configuration.
class-of-service	Optional. Displays all voice class of service (CoS) configurations.
class-of-service <*name*>	Optional. Displays voice CoS configurations for the specified rule set.
directory	Optional. Displays voice directory configuration.
grouped-trunk	Optional. Displays all voice trunk group configurations.
grouped-trunk <*name*>	Optional. Displays voice trunk group configurations for the specified trunk.
line	Optional. Displays the voice line configuration.
line <*number*>	Optional. Displays the voice line configuration for a specified extension.
mail	Optional. Displays voicemail configuration.
match	Optional. Displays all substitution configurations.
match ani	Optional. Displays ANI substitution configurations.
mgcp-endpoint	Optional. Displays all Media Gateway Control Protocol (MGCP) endpoint configurations.
mgcp-endpoint <*index*>	Optional. Displays a specific MGCP endpoint configuration.
music-on-hold	Optional. Displays all Music on Hold (MoH) configurations.
music-on-hold mode	Optional. Displays all MoH mode configurations.
music-on-hold player	Optional. Displays all MoH player configurations.
music-on-hold player <*name*>	Optional. Displays the MoH player configuration for the specified player.
named-digit-timeouts	Optional. Displays all named-digit-timeouts.
named-digit-timeouts <*name*>	Optional. Displays configuration for the specified named-digit-timeout.
operator-group	Optional. Displays operator group configuration.
paging-group	Optional. Displays all handset paging group configurations.
paging-group <*extension*>	Optional. Displays handset paging group configuration for the specified paging group.
pickup-group	Optional. Displays all call pickup group configurations.

pickup-group <*name*>	Optional. Displays call pickup group configuration for the specified call pickup group.
queue	Optional. Displays all call queue configurations.
queue <*extension*>	Optional. Displays call queue configuration for the specified call queue.
ring-group	Optional. Displays all configured ring groups.
ring-group <*name*>	Optional. Displays ring group configurations for the specified ring group.
ring-option	Optional. Displays all ring option configurations.
ring-option <*name*>	Optional. Displays ring option configurations for the specified ring option.
speed-dial	Optional. Displays all entries for speed-dial entries.
spre	Optional. Displays entire special prefix (SPRE) related configuration, including mode, overrides, local maps, and network template.
spre-map	Optional. Displays only the SPRE mapping configuration.
status-group	Optional. Displays all status group information.
status-group <*name*>	Optional. Displays information on the specified status group.
trunk	Optional. Displays all voice trunk configurations.
trunk <*Txx*>	Optional. Displays voice trunk configurations for the specified trunk. Use the trunk's two-digit identifier following T (for example, **T99**).
trunk-list	Optional. Displays all trunk list configurations.
trunk-list <*name*>	Optional. Displays a specific trunk list configuration.
user	Optional. Displays all configured voice users.
<*number*>	Optional. Displays voice user configurations for the specified number.
<*name*>	Optional. Displays voice user configurations for the specified name. Enter the first or last name.
<*last name*>	Optional. Displays voice user configurations for the specified name. Enter the last name only.
verbose	Optional. Displays detailed information on all or on the specified voice running configurations.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded.
Release 13.1	Command was expanded.
Release 14.1	Command was expanded.
Release 15.1	Command was expanded.
Release 16.1	Command was expanded.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include** parameters.

Release A2	Command was expanded to include the **ani-list**, **match**, **mgcp-endpoint**, **named-digit-timeouts**, **trunk-list**, and **user** parameters.
Release A2.03	Command was expanded to include the **spre** and **spre-map** parameters.
Release A2.04	Command was expanded to include the **paging-group** parameter.
Release A4.01	Command was expanded to include the **pickup-group** parameter, **voice queue**, and **music-on-hold**.
Release R10.7.0	Command was expanded to include the **ring-option** parameter.

Usage Examples

The following is sample output from the **show running-config voice** command:

```
>enable
#show running-config voice
Building configuration...
!
voice hold-reminder 15
voice flashhook mode interpreted
!
voice dial-plan 1 local 8000
!
voice class-of-service set1
 billing-codes
!
voice class-of-service set2
!
voice class-of-service “set 1"
!
voice codec-list trunk
 default
 codec g711ulaw
 codec g729
!
voice codec-list “list 1"
!
voice codec-list list1
!
voice trunk T99 type t1-rbs supervision wink role network
!
voice trunk T01 type sip
!
voice trunk T07 type t1-rbs supervision wink role network
!
voice trunk T02 type t1-rbs supervision wink role network
!
--MORE--
```


show schedule

Use the **show schedule** command to display information regarding the schedule configuration.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show schedule** command:

```
>enable
#show schedule
Schedule entry: DELAY-AFTER-BOOT (active)
Schedule entry: DELAY (inactive)
```

Technology Review

The scheduler provides a method for configuring a feature to operate during a specific time schedule and to receive feedback when the feature should disable or enable. The goal of the scheduler is to eliminate redundant code while providing an understandable, streamlined application program interface (API) for rapid feature development with schedules. The **show schedule** command displays how many features are scheduled and whether they are active or inactive.

show sfp-info interface *<interface>*

Use the **show sfp-info interface gigabit-switchport** command to display small form-factor pluggable (SFP) transceiver module serial ID information for the specified interface.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<interface>	Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show spanning-tree interface ?** for a complete list of valid interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 17.6	Command was introduced.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Functional Notes

Fields in the **show** command output reported as **Unspecified** are not applicable to the module type. Refer to the *Usage Examples* for more information.

Usage Examples

The following is sample output from the **show sfp-info interface gigabit-switchport** *<slot/port>* command:

```
>enable
#show sfp-info interface gigabit-switchport 0/25

SFP Manufacturer: FINISAR CORP.
  Identifier: SFP Transceiver
  Connector: LC
  SONET Compliance Code: Unspecified
```


Gigabit Ethernet Compliance Code: 100BASE-SX
Fiber Channel Link Length: Intermediate Distance <I>
Fiber Channel Transmitter Technology: Shortwave laser w/o OFC <SN>
Fiber Channel Transmitter Media: Multi-Mode, 62.5m <M6>
Fiber Channel Speed: 200 MB/sec
Encoding: 8B10B
Nominal Bit Rate: 2100 Mb/s
Supported Single-Mode Link Length <Km units>: Unspecified
Supported Single-Mode Link Length <100m units>: Unspecified
Supported Multi-Mode <50micron> Link Length <10m units>: 30
Supported Multi-Mode <62.5micron> Link Length <10m units>: 15
Supported Link Length Copper: Unspecified
Vendor OUI: 00:90:65
Vendor Part Number: FTRJ8519P1BNL
Vendor Revision: A
Options: LOS, TX_DISABLE
Bitrate, Max: Unspecified
Bitrate, Min: Unspecified
Vendor Serial Number: PA41HCB
Datecode: Jul 31. 2005

show sfp-info summary

Use the **show sfp-info summary** command to display a summary of all of the small form-factor pluggable (SFP) transceiver modules currently installed in the unit.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

This command displays the interface in which the module is installed, the manufacturer of the module, and, if supported, the Rx power, Tx power, and temperature.

Usage Examples

The following is sample output from the **show sfp-info summary** command:

```
>enable
#show sfp-info summary
```

Interface	SFP Manufacturer	Rx Power	Tx Power	Temperature
xgiga-swx 1/2/1	OPNEXT, INC.	0.56mW	0.57mW	33 Celsius
xgiga-swx 4/2/1	MergeOptics GmbH	0.67mW	0.45mW	37 Celsius
xgiga-swx 4/2/1	OPNEXT, INC.	0.63mW	0.57mW	34 Celsius
xgiga-swx 5/2/1	FCI MergeOptics	0.59mW	0.64mW	34 Celsius
xgiga-swx 5/2/2	Molex Inc.	mW	mW	Celsius
xgiga-swx 6/2/1	Molex Inc.	mW	mW	Celsius
xgiga-swx 6/2/2	Axcen Photonics	0.15mW	0.00mW	26 Celsius

show sftp sftp-client mypubkey

Use the **show sftp sftp-client mypubkey** command to display the Secure File Transfer Protocol SFTP secure shell (SSH) public key information.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R13.11.0	Command was introduced.

Usage Examples

The following example displays SFTP SSH DSA and RSA public key hashes:

```
>enable
#show sftp sftp-client mypubkey

DSA Hash: ---- BEGIN SSH2 PUBLIC KEY ----
Comment: Adtran DSA Public key
AAAAB3NzaC1kc3MAAAEBALq7iC0mltbBGo2EzQ3ZDekHl3t2DLa08mP1AxrDdZdl
0HPTjHbVWrLOFnd3Om2yv8LXrKIKnlM0GhMlAB6ZcDjQjyr8s/Ey9fLZmxBdYKt3
8GP0OFLk2zEeYRv6XzFIYAu1sbcfmTU18SV+9m3X+TkhKvP/1jKYSSwDRyNDYTWJ
9Ap+HLRY09tLIvn9cL9mwDCG1rNSlsZ+y0uuYGOwGECLfCxuPc9gZbtMzdd6URqz
tze37XZTBOKyvz2AQrjRux9LNp13DZOB+R1SzNw2fhbPxalzeOXVVLxA7Gvty3YX
8PtyDfxu8KOqNIUVkhXxFf3OJMSyoXSCKC6GPIgxQSkAAAAVANrLmgntjpU7H2Ln
4jFsjjRekvP1AAABAGc4rfqF1ivIJ+AZlRlYRmtjk47zoZ2AU7alotVnaM8jK+U7
qJOWccGZeIUl69Y7xOZ9H3QG0W+LD4bpERJVCrUQxWWxdITOIphAM/OIeIcE1czW
tDUemFoAeg503n9rQuvNiSQ5+qhVsGWC9zhdo4AAZ2Crw/Epn54K778rpDjvzxcW
sesX7Vp3tsXHbZ6RGxdqFCJHytY0xNj033RaKSeAq4aZwbUMCYmrb1iS1hl1CHYM
b1kTsd7MYZQQ12e5UvVPySSNrN1R4ocDQy5qDi/UC5HfKe5MdLp5tM9ZWAjipDGk
3XjKO6UKMPT9cPa6iZ1fUXgwnam7xOSwtFU1HiEAAAEBAJ4bnLz7NxH3lTxn3e62
t+Qhgzri17tM9sl3B3yMWNv4h0EiFkM/9k+4zOBYan3JUt7VQnuxZ7DYkPeymE6h
ZML4QYBhSNMoW6SSseDuF52zGOk48tD9MzbBb/OabmIlmCwlRbiaYCzC0/ZNUaZs
```


ZhWGiNSbzR9As8qzYz4Hyr2EFImkgmO4zSV53u//hIXtNKgrTxmh73PFixaX86op
9nty+Ivva8iNDu1yRfLsd7XZeHjgcMymsgQEwKeU/0AhSJJ1rCIB83WA8eESCbSo
IZokzb0kreD+g+kbSfWFDXy16L9YpzOeUj6096e/fUMD/Dv8PNt5Ql7+imZ+HmHw
VuI=
---- END SSH2 PUBLIC KEY ----

RSA Hash: ---- BEGIN SSH2 PUBLIC KEY ----
Comment: Adtran RSA Public key
AAAAB3NzaC1yc2EAAAABAwAAAQEA+OYNfxP0JhhrTomlfnu+dxztHWoZRzCLTKbP
SGAC5NxsoXHQhVW8TOSpIv4KXDjhUnD0EGza8oDcdBjwOKVgQetcx55oL16NRIWj
Tm8oLBQXx+KlksSNvlx5jEZDen5ZxHKs6WiFc6OgV3+Xn/zJWeKopm8YpbxkIZoR
XIwsJlhWFLKwuZH2q9DNhkLiuR2PbTDvV/qTnG2Qd/SLYZRPs9N8/LZjeZWCDyEo
pEHRrN6SnAxLoifJThpbDNsVXrS/x++iXOiDDulNiUoaFWbnWaM2bdI360Frp/FI
miz6vf5LAOzZ7hsT+tQzLCcHM/cjPAr9JCA+9YrZgIMJcv45qw==
---- END SSH2 PUBLIC KEY ----

show shaper

Use the **show shaper** command to display configuration information for Ethernet virtual connection (EVC) traffic shapers. Variations of this command include:

show shaper

show shaper <*name*>

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*name*>	Optional. Specifies that information for a single traffic shaper is displayed.

Default Values

By default, no traffic shapers are configured.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display information for all configured EVC traffic shapers:

>**enable**
#show shaper

Name	State	Status
1	Disabled	Disabled

Attributes:
    Configured Rate : 1000000 kbps
    Mode : Not applied

show sip

Use the **show sip** command to display Session Initiation Protocol (SIP) statistical and registration information. Variations of this command include:

show sip auxiliary-transactions
show sip resources
show sip statistics
show sip user-registration
show sip user-registration *<user>*
show sip user-registration detail
show sip user-registration user-agent

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

auxiliary-transactions	Displays SIP auxiliary transaction information.
resources	Displays SIP server resource information.
statistics	Displays SIP server statistic information.
user-registration	Displays local SIP server registration information for all users.
<user>	Optional. Displays local SIP server registration information for the specified user.
detail	Optional. Displays a detailed listing of the local SIP server registration information for all users.
user-agent	Optional. Displays the SIP user agent information for all users.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 11.1	**Resources**, **statistics**, and **user-registration** parameters were added.
Release 15.1	**Name-service name-table** parameter was added.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.3	Command was altered to remove the **name-service name-table** parameter, which was replaced with the **show voip name-service name-table** command.

Release R10.5.0	Command was expanded to include the **auxiliary-transactions** parameter.
Release R10.8.0	Command was expanded to include the <*user*>, **detail**, and **user-agent** parameters.

Usage Examples

The following is sample output from the **show sip statistics** command:

```
>enable
#show sip statistics

Invites transmitted: 36
Invites received: 26

Invite Retransmits transmitted: 11
Invite Retransmits received: 0
Non-Invites transmitted: 1869
Non-Invites received: 1911

Non-Invite Retransmits transmitted: 12
Non-Invite Retransmits received: 41

Responses transmitted: 1982
Responses received: 3535

Response Retransmits transmitted: 45
Response Retransmits received: 0
```

The following is sample output from the **show sip user-registration** command:

```
>enable
#show sip user-registration

User            IP Address      Port        Transport   Expires
-------------------------------------------------------------------------------------------------
9001            10.10.10.1      5060        UDP         2081
9002            10.10.10.2      5060        UDP         3419

Total phones registered: 2
```

show sip location

Use the **show sip location** command to display Session Initiation Protocol (SIP) statistical and registration information. Variations of this command include:

show sip location
show sip location dynamic
show sip location static

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

dynamic	Optional. Displays SIP location database dynamic entries.
static	Optional. Displays SIP location database static entries.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command output was updated.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show sip location static** command:

```
>enable
#show sip location static
User       IP Address     Port     Expires     Source
-------------------------------------------------------------------------
9001       1.1.1.2        5060     52          Registrar
9002       10.10.10.2     5060     3336        Registrar
```


show sip proxy

Use the **show sip proxy** command to display Session Initiation Protocol (SIP) proxy statistical and registration information. Variations of this command include:

show sip proxy monitor
show sip proxy registration
show sip proxy registration extended
show sip proxy registration range *<range>*
show sip proxy registration range *<range>* **extended**
show sip proxy registration range *<range>* **realtime**
show sip proxy registration realtime
show sip proxy registration user *<user>*
show sip proxy registration user *<user>* **extended**
show sip proxy registration user *<user>* **realtime**
show sip proxy registration verbose
show sip proxy resources
show sip proxy resources realtime
show sip proxy user
show sip proxy user extended
show sip proxy user realtime
show sip proxy user verbose

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

monitor	Displays SIP proxy monitor status.
registration	Displays the SIP Proxy registration status for SIP proxy users.
range *<range>*	Optional. Specifies a range of consecutive extensions to display, for example, **2565551000-2565551200**.
user *<user>*	Optional. Specifies a single user extension to display.
resources	Displays SIP proxy resource information.
user	Displays SIP proxy user database information.
extended	Optional. Displays the extended form of SIP proxy user database.

realtime	Optional. Displays SIP proxy information in real time. Refer to the *Functional Notes* below for more information.
verbose	Optional. Activates detailed debug messages.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.3	Command was expanded to include the **extended** modifier.
Release A2.03	Command was expanded to include the **verbose** modifier.
Release A5.02	Command was expanded to include the **registration**, **range** <*range*>, and **user** <*user*> parameters.
Release R10.9.0	Command was expanded to include the **monitor** parameter.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show sip proxy monitor** command:

```
>enable
#show sip proxy monitor

Proxy Server Monitor:              Admin UP
Polling mode:                      On failure
Continuous interval:               30
Delay:                             Min <min> Max <max> | Disabled
Recovery no-response interval:     5 - 60
Recovery responses needed:         3  Interval 10

Servers:
Address                            Port        Status      Poll
---------------------------------- ------      --------    -------------------
10.255.3.2                         5060        DOWN        Next poll 12 seconds
10.17.233.254                      5060        UP*
```


10.17.1.254 5060 UP

The following is sample output from the **show sip proxy resources** command:

>**enable**
#show sip proxy resources

Type	Name	Allocated	Currently in Use	Max Used
Proxy	proxyPoolElements	630	0	0

show sip secure remote-user

Use the **show sip secure remote-user** command to display Session Initiation Protocol (SIP) security statistics pertaining to remote users attempting to access the system. Variations of this command include:

show sip secure remote-user
show sip secure remote-user blacklist
show sip secure remote-user dropped-requests

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

blacklist	Optional. Displays UDP SIP security blacklist entries.
dropped-requests	Optional. Displays UDP SIP security dropped requests due to failed authentication attempts.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

These statistics display the number of dropped SIP requests and the type, such as REGISTER and INVITE, that were encountered on the configured secure port. Other requests include ACK, CANCEL, OPTIONS, SUBSCRIBE, NOTIFY, PUBLISH, INFO, REFER, MESSAGE, and UPDATE requests. The output also displays the number of suspect entries with summary information which includes the IPv4 address and voice user attempting a call. Once the number of failed attempts from an IPv4 address, regardless of its source port, exceeds the blacklist attack threshold, a blacklist entry is recorded and the IPv4 address is removed from the suspect list.

A maximum number of 100 combined entries can be stored in the suspect and blacklist entry tables. If the maximum number is exceeded, the oldest entries from the suspect list are removed as needed to make room for new blacklist entries, and no new suspect entries are added. When there are no suspect entries left to sacrifice for space, no more blacklists entries will be added until blacklist entries are removed either manually (using the command *clear sip secure remote-user on page 207*) or through timeouts.

Usage Examples

The following is sample output from the **show sip secure remote-user** command:

>**enable**
#show sip secure remote-user

Dropped SIP Request Information:

Port	Protocol	Registers	Invites	Other Requests
2112	UDP	0	33	0

Number of secure ports: 1
Suspect Entries:
10.10.23.2 : 2112 / UDP
  User/Agent: 2565551234/Adtran-SIP-IP706/v2.4.0.3
  Timeout (seconds): 600
Total suspect entries: 1

Blacklisted Entries:
10.10.19.1 : 2112 / UDP
  User/Agent: 2565556789/Adtran-SIP-IP706/v2.4.0.3
  Timeout (seconds): 3600
Total blacklisted entries: 1

* Port, protocol, and User/Agent values taken from first suspect SIP message

show sip trunk-registration

Use the **show sip trunk-registration** command to display Session Initiation Protocol (SIP) statistical and registration information. Variations of this command include the following:

show sip trunk-registration
show sip trunk-registration realtime
show sip trunk-registration registrar
show sip trunk-registration subscription
show sip trunk-registration verbose
show sip trunk-registration registrar realtime
show sip trunk-registration registrar <*Txx*>
show sip trunk-registration registrar <*Txx*> **realtime**
show sip trunk-registration registrar <*Txx*> <*name*>
show sip trunk-registration registrar <*Txx*> <*name*> **realtime**
show sip trunk-registration subscription <*Txx*>
show sip trunk-registration subscription <*Txx*> **realtime**
show sip trunk-registration subscription <*Txx*> <*name*>
show sip trunk-registration subscription <*Txx*> <*name*> **realtime**
show sip trunk-registration <*Txx*>
show sip trunk-registration <*Txx*> **realtime**
show sip trunk-registration <*Txx*> <*name*>
show sip trunk-registration <*Txx*> <*name*> **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<*Txx*>	Optional. Specifies the trunk identity; where xx is the trunk's two-digit identifier (e.g., T01).
<*name*>	Optional. Specifies the name associated with the trunk.
realtime	Optional. Displays local SIP client registration information in real time. Refer to the *Functional Notes* below for more information.
registrar	Optional. Displays the SIP trunk registrar IP address information. Refer to the *Functional Notes* below for more information.

subscription	Optional. Displays SIP trunk registration subscription information.
verbose	Optional. Displays detailed SIP trunk registration information.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A5.01	Command was expanded to include the **registrar** parameter
Release R13.4.0	Command was expanded to include the **verbose** parameter.
Release R13.8.0	Command was expanded to include the **subscription** parameter.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the command *terminal length <number> on page 1133*).

Use the **registrar** to show the ip address of the registrar that each number is using on a SIP trunk. Numbers on the same SIP trunk can use different registrars if sip-server validation is enabled (using the command *sip-server validation register on page 5140*).

Usage Examples

The following is sample output from the **show sip trunk-registration** command:

```
>enable
#show sip trunk-registration

Ext     Register  Expire    Grant    Success  Redirect  Challenge  Failed  Timeout
-------------------------------------------------------------------------------------------------------------
4433    NO        0         0        0        0         0          0       #
```

show smdr

Use the **show smdr** command to display the statistics for station message detail record (SMDR) reporting. The output for this command includes each item from the configured SMDR output format (refer to the command *voice logging smdr format on page 1929*).

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example is sample output from the **show smdr** command:

```
>enable
#show smdr
SMDR Formatting:
CALLID[10]
Date(MM/DD/YYYY)[10]
Start Time(HH.MM.SS)[8]
Billable Mins[6]
Billing Code[4]
Call Type[2]
Originating Slot[2]
Originating Port[2]
Originating Name[15]
Originating Number[15]
Destination Slot[2]
Destination Port[2]
Destination Name[15]
Destination Number[15]
Conference ID[3]
```


show snmp

Use the **show snmp** command to display the system Simple Network Management Protocol (SNMP) current configuration. Variations of this command include the following:

show snmp engineID
show snmp group
show snmp user

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

engineID	Displays the hex string that defines the current local engine ID settings.
group	Displays the list of all groups entered.
user	Displays the list of all users entered.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 13.1	Command was expanded to include the **engineID**, **group**, and **user** options.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show snmp** command for a system with SNMP disabled, and the default chassis and contact parameters:

```
>enable
#show snmp
Chassis: Chassis ID
Contact: Customer Service
0 Rx SNMP packets
  0 Bad community names
  0 Bad community uses
  0 Bad versions
  0 Silent drops
```


The following is sample output from the **show snmp group** command for a situation in which a group called **securityV3auth** was defined (via the **snmp-server group** command) using version 3 and authentication, and no access control list:

```
>enable
#show snmp group
Group: securityV3auth                Security Model: v3
Read View: default                   Write View: <not specified>
Notify View: default
```

show sntp

Use the **show sntp** command to display the system Simple Network Time Protocol (SNTP) parameters and current status of SNTP communications.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays the SNTP parameters and current status:

```
>enable
#show sntp
```


show spanning-tree

Use the **show spanning-tree** command to display the status of the spanning-tree protocol. Variations of this command include:

show spanning-tree
show spanning-tree <*number*>
show spanning-tree detail
show spanning-tree detail active
show spanning-tree realtime
show spanning-tree <*number*> **realtime**
show spanning-tree summary

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command may adversely affect system performance and should be used with discretion.*

Syntax Description

<*number*>	Optional. Displays spanning tree for a specific bridge group. This command is only applicable to routers configured for bridging.
detail	Optional. Displays detailed spanning tree information.
active	Optional. Displays detailed information about all active interfaces.
realtime	Optional. Displays full-screen spanning tree information in real time.
summary	Optional. Displays a summary of all port states.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 10.1	Command was expanded to include the **realtime** parameter.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.5	Command was expanded to include the **detail**, **active**, and **summary** keywords.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show spanning-tree** command:

```
>enable
#show spanning-tree
Spanning Tree enabled protocol ieee
 Root ID    Priority    32768
            Address     00:a0:c8:00:88:41
            We are the root of the spanning tree
            Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID Priority    32768
            Address     00:a0:c8:00:88:41
            Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time  300
Interface       Role    Sts     Cost    Prio. Nbr.  Type
eth 0/2         Desg    FWD     19      128.2       P2p
eth 0/3         Desg    FWD     19      128.3       P2p
eth 0/4         Desg    FWD     19      128.4       P2p
giga-eth 0/1    Desg    FWD     4       128.25      P2p
giga-eth 0/2    Desg    FWD     4       128.26      P2p
```


show spanning-tree active

Use the **show spanning-tree active** command to display the spanning-tree status on active interfaces only. Variations of this command include:

show spanning-tree active
show spanning-tree active detail

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

detail	Optional. Displays the spanning-tree protocol status in detail.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show spanning-tree active** command:

```
>enable
#show spanning-tree active
Spanning Tree enabled protocol ieee
 Root ID    Priority    32768
            Address     00:a0:c8:00:88:41
            We are the root of the spanning tree
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID Priority    32768
            Address     00:a0:c8:00:88:41
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time   300
eth 0/9         Desg FWD 19        128.9   P2p
eth 0/2         Desg FWD 19        128.24  P2p
--MORE--
```


show spanning-tree blockedports

Use the **show spanning-tree blockedports** command to display ports that are currently in a blocked state.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show spanning-tree blockedports** command:

```
>enable
#show spanning-tree blockedports
Blocked Interfaces List
-----------------------------------
eth 0/3
giga-eth 0/2
p-chan 1
Number of blocked ports (segments) in the system: 3
```


show spanning-tree interface <*interface*>

Use the **show spanning-tree interface** command to display spanning-tree protocol information for a particular interface. Variations of this command include:

show spanning-tree interface <*interface*>
show spanning-tree interface <*interface*> **active**
show spanning-tree interface <*interface*> **active detail**
show spanning-tree interface <*interface*> **cost**
show spanning-tree interface <*interface*> **edgeport**
show spanning-tree interface <*interface*> **inconsistency**
show spanning-tree interface <*interface*> **priority**
show spanning-tree interface <*interface*> **rootcost**
show spanning-tree interface <*interface*> **state**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*interface*>	Specifies an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **show spanning-tree interface ?** for a complete list of valid interfaces.
active	Optional. Displays information for an active interface.
active detail	Optional. Displays detailed spanning-tree protocol information for an active interface.
cost	Optional. Displays only spanning-tree protocol path cost information.
edgeport	Optional. Displays information for all interfaces configured as edgeports.
inconsistency	Optional. Displays information for all interfaces with port inconsistencies.
priority	Optional. Displays only spanning-tree protocol priority information.
rootcost	Optional. Displays only spanning-tree protocol root path cost information.
state	Optional. Displays only spanning-tree protocol state information.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R10.10.0	Command was expanded to include the **inconsistency** parameter.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following is sample output from the **show spanning-tree interface ethernet** command:

```
>enable
#show spanning-tree interface ethernet 0/2
Interface          Role               Sts              Cost       Prio. Nbr.  Type
------------------ ------------------ ---------------- ---------- ----------- ---------------
eth 0/2            Desg               LIS               19         128.2       P2p
```

show spanning-tree pathcost method

Use the **show spanning-tree pathcost method** command to display the default pathcost method being used.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show spanning-tree pathcost method** command. In this case, 32-bit values are being used when calculating path costs:

```
>enable
#show spanning-tree pathcost method
Spanning tree default pathcost method used is long
```


show spanning-tree root

Use the **show spanning-tree root** command to display information regarding the spanning-tree protocol root. Variations of this command include:

show spanning-tree root
show spanning-tree root address
show spanning-tree root cost
show spanning-tree root detail
show spanning-tree root forward-time
show spanning-tree root hello-time
show spanning-tree root id
show spanning-tree root max-age
show spanning-tree root port
show spanning-tree root priority
show spanning-tree root priority system-id

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

address	Optional. Displays the address of the spanning-tree root.
cost	Optional. Displays the path cost of the spanning-tree root.
detail	Optional. Displays the spanning-tree root information in detail.
forward-time	Optional. Displays the forward-time of the spanning-tree root.
hello-time	Optional. Displays the hello-time of the spanning-tree root.
id	Optional. Displays the ID of the spanning-tree root.
max-age	Optional. Displays the maximum age of the spanning-tree root.
port	Optional. Displays the port of the spanning-tree root.
priority	Optional. Displays the priority of the spanning-tree root.
priority system-id	Optional. Displays the priority and system-id of the spanning-tree root.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show spanning-tree root** command:

```
>enable
#show spanning-tree root
Root ID                 Root Cost   Hello Time  Max Age    Fwd Dly     Root Port
----------------------  ----------  ----------  ---------  ----------  ----------------
8191 00:a0:c8:b9:bb:82  108         2           20         15          eth 0/1
```

show srtp media sessions

Use the **show srtp media sessions** command to display media sessions that were negotiated to use Secure Realtime Transfer Protocol (SRTP) and to display key information about the SRTP session.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example displays information about SRTP media sessions:

```
>enable
#show srtp media sessions
-----------   ---- ----   -----   ------------------------
     |   SRTP | SRTCP |
   Call ID | Auth Encr | Encr  | Crypto
-----------   ---- ----   -----   ------------------------
        1       Yes  Yes    Yes     AES_CM_128_HMAC_SHA1_80
   Anchored: 10.19.247.5:10000
   Remote:   10.100.254.4:19888

        1   Yes  Yes    Yes     AES_CM_128_HMAC_SHA1_80
   Anchored: [::]:10002
   Remote:   127.0.0.1:10002

        1   Yes  Yes    Yes     AES_CM_128_HMAC_SHA1_80
   Anchored: 10.19.247.5:10001
   Remote:   10.100.254.4:19889

There are 3 active media sessions.
```


show ssh port-forward

Use the **show ssh port-forward** command to display a summary of secure shell (SSH) port forward information.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.4.0	Command was introduced.

Usage Examples

The following is sample output from the **show ssh port-forward** command:

```
>enable
#show ssh port-forward
Local Port: 22
URL of Remote User: AOS@10.23.153.22:5037
Status: Waiting for Connection
```

> *If the port forward has an active connection, the status will display as **Forwarding** instead of **Waiting for Connection**.*

show ssh-server

Use the **show ssh-server** command to display the system's public key for secure shell (SSH) connections. Variations of this command include:

show ssh-server detail
show ssh-server key-hash
show ssh-server key-hash rsa-sha2-512
show ssh-server mypubkey <*SSH public key fingerprint*>
show ssh-server mypubkey fingerprint <*fingerprint of SSH server public key*>
show ssh-server mypubkey fingerprint md5
show ssh-server mypubkey fingerprint sha1
show ssh-server mypubkey fingerprint sha2

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Displays the configured SSH server security parameters used for established SSH connections.
key-hash	Displays the SSH server public key hash of a given key string in SHA1 Digital Signature Standard (DSS) format.
rsa-sha2-512	Displays the SSH server public key hash of a given key-string in SHA-2 format.
mypubkey	Specifies displaying the SSH server public key.
fingerprint md5	Specifies displaying the MD5 fingerprint of SSH server public key.
fingerprint sha1	Specifies displaying the SHA1 fingerprint of SSH server public key.
fingerprint sha2	Specifies displaying the SHA2 fingerprint of SSH server public key.

Default Values

No default values are necessary for this command.

Command History

Release R14.4.0	Command was expanded to include rsa-sha2-512, fingerprint sha2.

Usage Examples

The following is sample output from the **show ssh-server** command:

>**enable**
#show ssh-server mypubkey
---- BEGIN SSH2 PUBLIC KEY ----
Comment: Adtran DSA Public key
AAAAB3NzaC1kc3MAAACBAKZf6qtRHGHjPfOP3drwO1m28l4fpN5X5c8ArkeKhV3a
TzY404uwCsSvfYQUw/s24E+989MWZxLUO0Ib+nV+hWlK0nxI85bQPIvOjaWNtbgg
OfNdz4VyNcLxxzsiJqNhQpGQ3LW2zQ7fsP9pM5ALAs7MDOaSdNja58aUgEMY1ta5
AAAAFQC1r9L5Mkax780fOnwkDB6eIaNjCwAAAH97vSxdyRel4IucL4Ckn7Y/zVwF
eLpwHiVP41MN7dO2aApuWvsygLU/FUAouv/3PRug/bAAS56w2/JLKVvyo1aRPNHA
vgPFEDodqLc+dnC1bXFu1VR69ntQYTEe6iReLlwzeEPLwTW5ucGHddXVbP2jG3R+
JEmGGt87P3JxicCjAAAAgAajR0ptcBY1jOye/kO8soQz/Dv2FqO4tW/yjFaV0E1J
v+vyAMUKUgocqebciS9RofjRTZ7W153z6JIpoFRnpOC+ynIVrBRUD+/1BgqJTI6G
0VtKm6A/K+qSaSd6dhKOAAWA1C0zsJDSkhKqYwRa1ziNC7TUFHIj/n1OvIo1PdzC
---- END SSH2 PUBLIC KEY ----

The following is sample output from the **show ssh-server** command:

>**enable**
#show ssh-server mypubkey fingerprint md5

DSA Hash: 9e:50:3c:8c:a2:7b:c7:8a:75:36:ce:78:8c:6c:bd:bb

RSA Hash: b3:c8:b4:07:72:f1:70:1b:a1:90:3e:6d:2a:6c:02:b2

ECDSA NISTP256 Hash: 62:0f:bd:98:77:3c:0e:1e:1a:37:a8:9a:2b:31:73:0c

ECDSA NISTP384 Hash: 27:3e:3d:3b:c0:63:71:2b:7b:fd:6b:43:ca:67:e0:bc

ECDSA NIST521 Hash: 55:a5:65:53:b1:f5:a3:3e:3b:0f:cf:fe:3f:18:39:1c

show ssh-client

Use the **show ssh-client** command to display the system's public key for secure shell (SSH) connections. Variations of this command include:

show ssh-client detail | <begin/exclude/include>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Displays the configured SSH server security parameters used for established SSH connections.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.
Release R13.12.0	Command was expanded to include the **detail** parameter.

Usage Examples

The following example displays the configuration of the show ssh-client command:

```
>enable

#show ssh-client detail | <text>

Server IP - 10.49.228.61
Client IP - 10.49.121.2
Client version string : SSH-2.0-libssh2_1.9.0
Negotiated kex algorithm : diffie-hellman-group14-sha1
Negotiated host key format: ssh-rsa
Negotiated encryption algorithm (client to server) : aes128-crt
```


Negotiated encryption algorithm (server to client) : aes128-crt
Negotiated MAC algorithm (client to server) : hmac-sha2-256
Negotiated MAC algorithm (server to client) : hmac-sha2-256
Negotiated compression algorithm (client to server) : None
Negotiated compression algorithm (server to client) : None
SSH authentication method : password

show stack

Use the **show stack** command to view the status of all the switches configured for stacking. Displays the mode of the switch as either master or member. If the mode is master, this command also gives the status of the stack members. Variations of this command include:

show stack
show stack candidates
show stack candidates realtime
show stack realtime
show stack topology
show stack topology realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

candidates	Optional. Displays all units that have registered with this stack master. This option is only available on a switch configured as a stack master.
topology	Optional. Displays the stack topology. This option is only available on a switch configured as a stack master.
realtime	Optional. Displays full-screen output in real time. Refer to *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

The stack candidates are a list of units that could be added to the stack. They are not yet members.

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example displays the configuration of the switch stack while in stack-master mode:

```
>enable
#show stack
Stack mode is MASTER
 Management Vlan is 2386, firmware version is 08.00.18.D
 Stack network is 169.254.0.0/24

Stack members...
Member   Mac Address          Mgmt IP Address   Source Interface   State
2        00:A0:C8:02:CF:C0    169.254.0.2       Stack port         Up
3        00:A0:C8:00:8C:20    169.254.0.3       Stack port         Up
#
```

Member	Specifies the stack member's Unit ID.
Mac Address	Specifies the stack member's medium access control (MAC) address.
Mgmt IP Address	Specifies the stack member's IP address.
Source Interface	Specifies the interface that the stack member was learned from.
State	Specifies the stack member’s state: **Up** (member is up and functioning properly); **Down** (member was at one time functioning, but contact has been lost); **Waiting** (waiting for the unit to register; when registered, it will be added to the stack); **Denied** (the unit could not be added to the stack because the stack protocol versions were not compatible).

The following example displays the configuration of the switch stack while in stack-member mode:

```
>enable
#show stack
Stack mode is STACK-MEMBER
 My Unit ID is 3, management Vlan is 2386
 Stack management network is 169.254.0.0/24
Stack Master info:
 Master is “Switch”, learned via giga-eth 0/1
 IP address is 169.254.0.1, MAC address is 00:DE:AD:00:65:83
#
```


The following example displays all units that have registered with this stack-master:

>**enable**
#show stack candidates
Displaying all known Stack candidates...

MAC Address	System Name	Source Interface	AOS Revision
00:A0:C8:00:8C:20	LabSwitch1	stack port	08.00.18
00:A0:C8:00:F5:6C	LabSwitch2	stack port	08.00.19.D
00:A0:C8:02:CF:C0	LabSwitch3	stack port	08.00.20.D

#

show startup-config

Use the **show startup-config** command to display a text printout of the startup configuration file stored in nonvolatile random access memory (NVRAM). Variations of this command include:

show startup-config
show startup-config checksum

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

checksum	Optional. Displays the message digest 5 (MD5) checksum of the unit's startup configuration.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

This command is used in conjunction with the **show running-config checksum** command to determine whether the configuration has changed since the last time it was saved.

Usage Examples

The following is sample output from the **show startup-config** command:

```
>enable
#show startup-config
!
!
no enable password
!
ip subnet-zero
ip classless
ip routing
!
```



```
event-history on
no logging forwarding
logging forwarding priority-level info
no logging email
!
ip policy-timeout tcp all-ports 600
ip policy-timeout udp all-ports 60
ip policy-timeout icmp 60
!
!
!
interface eth 0/1
speed auto
 no ip address
 shutdown
!
interface dds 1/1
 shutdown
!
interface bri 1/2
 shutdown
!
!
ip access-list standard MatchAll
 permit host 10.3.50.6
 permit 10.200.5.0 0.0.0.255
!
!
ip access-list extended UnTrusted
 deny   icmp 10.5.60.0 0.0.0.255 any source-quench
 deny   tcp any any
!
no snmp agent
!
!
!
```

show storm-control interfaces *<interface>*

Use the **show storm-control interfaces** to display configuration parameters and current statistics for all interfaces configured with storm control. Variations of this command include the following:

show storm-control interfaces *<interface>* **broadcast burst**
show storm-control interfaces *<interface>* **broadcast rate**
show storm-control interfaces *<interface>* **multicast-unknown burst**
show storm-control interfaces *<interface>* **multicast-unknown rate**
show storm-control interfaces *<interface>* **unicast-unknown burst**
show storm-control interfaces *<interface>* **unicast-unknown rate**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<interface>	Specifies which interface information to display. Specify an interface in the format *<interface type [slot/port]>*. For example, for a Gigabit switchport interface, enter **gigabit-switchport 0/3**, or for a 10 Gigabit switchport enter **xgigabit-switchport 1/1**. Type **show storm-control interfaces ?** for a complete list of valid interfaces.
broadcast burst	Displays the configured burst rate for broadcast traffic.
broadcast rate	Displays the configured storm control rate for broadcast traffic.
multicast-unknown burst	Displays the configured burst rate for unknown multicast traffic.
multicast-unknown rate	Displays the configured storm control rate for unknown multicast traffic.
unicast-unknown burst	Displays the configured burst rate for unknown unicast traffic.
unicast-unknown rate	Displays the configured storm control rate for unknown unicast traffic.

Default Values

No default values are necessary for this command.

Command History

Release R11.8.0	Command was introduced.

Usage Examples

The following example displays storm control broadcast rate information for **gigabit-switchport 0/3**:

>**enable**
#show storm-control interfaces gigabit switchport 0/3 broadcast rate

show switchports

Use the **show switchports** command to display switchport information. Variations of this command include:

show switchports
show switchports vlans

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

vlans	Optional. Displays the switchport vlan membership.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following is sample output from the **show switchports** command:

```
>enable
#show switchports
Name: swx 0/1
Switchport: enabled
Administrative Mode: access
Negotiation of Trunking: access
Access Mode VLAN (configured): 1
Trunking Native Mode VLAN: 1
Trunking VLAN Enabled: 1-4094
Trunking VLAN GVRP Fixed: none
Port Expiration: disabled
Port Security: disabled
Protected: false
```


Name: swx 0/2
Switchport: enabled
Administrative Mode: access
Negotiation of Trunking: access
Access Mode VLAN (configured): 1
Trunking Native Mode VLAN: 1
Trunking VLAN Enabled: 1-4094
Trunking VLAN GVRP Fixed: none
Port Expiration: disabled
Port Security: disabled
Protected: false

show system

The **show system** command shows the system version, timing source, power source, and alarm relay status.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R12.1.0	Command output was modified for virtual AOS (vAOS) instances.

Functional Notes

In vAOS instances, the output of this command does not include checksum information, boot ROM or hardware versions, or boot system images names.

Usage Examples

The following is sample output from the **show system** command:

```
>enable
#show system
Adtran, Inc. OS version 07.00.20
 Checksum: 3B2FCC0F, built on Tue Jun 01 13:36:36 2004
Boot ROM version 07.00.20
 Checksum: 604D, built on: Tue Jun 01 13:59:11 2004
Copyright (c) 1999-2004, Adtran, Inc.
Platform: Total Access 900
Serial number TechPub
Flash: 8388608 bytes DRAM: 33554431 bytes
ICP uptime is 0 days, 0 hours, 53 minutes, 50 seconds
System returned to ROM by External Hard Reset
Current system image file is “070020.biz”
```


Boot system image file is “070020.biz”
Power Source: AC
Primary System clock source config: t1 0/1
Secondary System clock source config: t1 0/1
Active System clock source: t1 0/1

show system-control-evc

Use the **show system-control-evc** command to display configuration information for the system control Ethernet virtual connection (EVC). Variations of this command include:

show system-control-evc
show system-control-evc performance-statistics 15-minute
show system-control-evc performance-statistics 15-minute *<interval>*
show system-control-evc performance-statistics 24-hour
show system-control-evc performance-statistics 24-hour *<interval>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

performance-statistics	Optional. Displays performance statistics for the system control EVC.
15-minute	Displays cumulative performance statistics for the last 15 minutes.
24-hour	Displays cumulative performance statistics for the last 24 hours.
<interval>	Optional. Limits output to a range of historical intervals. Valid range is **1** to **96**.

Default Values

No default values necessary.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display configuration information for the system control EVC:

```
>enable
#show system-control-evc
System Control EVC
    S-TAG          : --
    Admin State    : Disabled
    EVC Status     : Connection not configured
    IP             : 0.0.0.0
    Subnet         : 255.255.255.255
    Connections    : None
```


System Control EVC Ethernet Info:
    0 packets input, 0 bytes
    0 unicasts, 0 broadcasts, 0 multicasts input
    0 unknown protocol, 0 discards
    0 input errors
    0 packets output, 0 bytes
    0 unicasts, 0 broadcasts, 0 multicasts output

show system-management-evc

Use the **show system-management-evc** command to display configuration information for the system management Ethernet virtual connection (EVC). Variations of this command include:

show system-management-evc
show system-management-evc performance-statistics 15-minute
show system-management-evc performance-statistics 15-minute *<interval>*
show system-management-evc performance-statistics 24-hour
show system-management-evc performance-statistics 24-hour *<interval>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

performance-statistics	Optional. Displays performance statistics for the system management EVC.
15-minute	Displays cumulative performance statistics for the last 15 minutes.
24-hour	Displays cumulative performance statistics for the last 24 hours.
<interval>	Optional. Limits output to a range of historical intervals. Valid range is **1** to **96**.

Default Values

No default values necessary.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

Enter the command as follows to display configuration information for the system management EVC:

```
>enable
#show system-management-evc
System Management EVC
    S-TAG          : --
    Admin State    : Disabled
    EVC Status     : SHUTDOWN
    IP             : 0.0.0.0
    Subnet         : 255.255.255.255
    Connections    : None
```


System Management EVC Ethernet Info:
    0 packets input, 0 bytes
    0 unicasts, 0 broadcasts, 0 multicasts input
    0 unknown protocol, 0 discards
    0 input errors
    0 packets output, 0 bytes
    0 unicasts, 0 broadcasts, 0 multicasts output

show system mtu

Use the **show system mtu** command to display the current system maximum transmission unit (MTU) setting.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.6	Command was introduced.

Usage Examples

The following is sample output from the **show system mtu** command:

```
>enable
#show system mtu

MTU size is 9216 bytes
```


show tacacs+ statistics

Use the **show tacacs+ statistics** command to display terminal access controller access control system (TACACS+) client statistics.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show tacacs+ statistics** command:

```
>enable
#show tacacs+ statistics
```

	Authentication	Authorization	Accounting
Packets sent:	0	0	0
Invalid responses:	0	0	0
Timeouts:	0	0	0
Average delay:	0ms	0ms	0ms
Maximum delay:	0ms	0ms	0ms
Socket Opens:	0		
Socket Closes:	0		
Socket Aborts:	0		
Socket Errors:	0		
Socket Timeouts:	0		
Socket Failed Connections:	0		
Socket Packets Sent:	0		
Socket Packets Received:	0		

show tcp info

Use the **show tcp info** command to display Transmission Control Protocol (TCP) control block information in AOS. This information is for troubleshooting and debug purposes only. For more detailed information, you can optionally specify a particular TCP control block. When a particular TCP control block is specified, the system provides additional information regarding crypto map settings that the **show tcp info** command does not display. Variations of this command include:

show tcp info
show tcp info realtime
show tcp info *<control block>*
show tcp info *<control block>* **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<control block>	Optional. Specifies a particular TCP control block for more detailed information.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show tcp info** command:

>**enable**
#show tcp info
TCP TCB Entries

ID	STATE	LSTATE	OSTATE	TYPE	FLAGS	RPORT	LPORT	SWIN	SRT	INTERFACE
0	FREE	FREE	FREE	SRVR	0	0	0	0	0	NONE
1	LISTEN	FREE	FREE	CONN	0	0	21	0	0	NONE
2	LISTEN	FREE	FREE	CONN	0	0	80	0	0	NONE
3	LISTEN	FREE	FREE	CONN	0	0	23	0	0	NONE
4	LISTEN	FREE	FREE	CONN	0	0	5761	0	0	NONE
5	FREE	FREE	FREE	SRVR	0	0	0	0	0	NONE

--MORE--

show tech

Use the **show tech** command to save technical information to a file named showtech.txt.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R12.1.0	Command output was modified for virtual AOS (vAOS) instances.

Functional Notes

The **show tech** command runs a script that creates a **showtech.txt** file in flash memory that contains the command output from the following show commands:

*Not all listed **show** commands apply to all Adtran products.*

show version
show modules
show flash
show cflash
show running-config verbose
show interfaces
show atm pvc
show dial-backup interfaces
show frame-relay lmi
show frame-relay pvc
show ip bgp neighbors

show ip bgp summary
show ip ospf neighbor
show ip ospf summary-address
show ip mroute
show ip bridge
show spanning-tree
show ip interfaces
show connections
show arp
show ip traffic
show tcp info
show ip protocols
show ip route
show ip access-lists
show event-history
show output-startup
show processes cpu
show buffers
show buffers users
show memory heap
show debugging

Usage Examples

The following example creates a **showtech.txt** file and displays it to the terminal screen:

>**enable**
#show tech
Opening and applying file.....
Done.

show temperature

Use the **show temperature** command to display the unit temperature.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show temperature** command:

```
>enable
#show temperature

Temperature: 33 degrees C
```


show thresholds

Use the **show thresholds** command to display thresholds currently crossed for all DS1 interfaces.

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show thresholds** command.

```
>enable
#show thresholds
t1 1/1:
    SEFS 15 min threshold exceeded
    UAS 15 min threshold exceeded
    SEFS 24 hr threshold exceeded
    UAS 24 hr threshold exceeded
t1 1/2:
    No thresholds exceeded
```


show timing-domain

Use the **show timing-domain** command to display the system timing domains.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following is sample output from the **show timing-domain** command:

```
>enable
#show timing-domain
Timing Domain Source Config Table
Domain          Interface       Config      Source      Status
    1           t1 0/1          Primary     Line        Alarm
    1           t1 0/2          None        System      Available
    2           t1 0/3          None        System      Available
    2           t1 0/4          Primary     Line        Alarm
Timing Domain System Config Table
Domain:  1      Active Source:  System
         Primary Interface      Source      Status
         t1 0/1                 t1 0/1      Alarm
         Secondary Interface    Source      Status
Domain:  2      Active Source:  System
         Primary Interface      Source      Status
          t1 0/4                t1 0/4      Alarm
         Secondary Interface    Source      Status
```


show tls profile

Use the **show tls profile** command to display the content of configured Transport Layer Security (TLS) profiles on the AOS device. Variations of this command include:

show tls profile
show tls profile <*name*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*name*>	Optional. Limits output to a single TLS profile.

Default Values

No default values necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example displays the content of the configured TLS profile **TLS_PROFILE1**:

```
>enable
#show tls profile TLS_PROFILE1
    Name: TLS_PROFILE1
    tls-version: 1.2
    authentication: server
    ca-profile:PROFILE1
    allow-self-signed-cert: no
    Identities Validated:
    ip-address
    fqdn configured
    Ciphersuite list:
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
    TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
    TLS_RSA_WITH_AES_256_CBC_SHA
    TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
```


TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
SSL_DES_192_EDE3_CBC_WITH_MD5

show tls sessions

Use the **show tls sessions** command to display information about each active Transport Layer Security (TLS) session.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example displays TLS session information:

```
>enable
#show tls sessions
    Application: SIP
    Version: TLS v1.2
    Ciphersuite: AES256-SHA
    Session ID: kKnKqvAM70IkGRBxzVHdVb8F8vkHpsL28A3D89xDGjA=
    Role: Client-only
    Local: 192.0.2.243:10459
    Peer: 198.51.100.4:5061
    Peer Certificate:
      Subject: CN = voip.example.com
      SAN IP Address:  2001:DB8:64FE::4 198.51.100.4  (Validated)
      SAN FQDN: ipv6.voip.example.com ipv4.ents.adtran.com voip.example.com  (Validated)

    There are 1 active TLS sessions.
```


show tls statistics

Use the **show tls statistics** command to display a summary of statistics for Transport Layer Security (TLS) configurations.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example displays a statistical summary for TLS configurations:

```
>enable
#show tls statistics
    TLS Connection Requests
    Total:2
    Passed:2
    Failed:0
    TLS Handshake
    Passed:2
    Failed:0
    TLS Connections
    Dropped:0
      Closed:1
```


show toneservices resources

Use the **show toneservices resources** command to display digital signal processor (DSP) tone information.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show toneservices resources** command:

```
>enable
#show toneservices resources

DSP  Channel  Type  Port  Status
-------------------------------------------------------------
 0/1   1      RTP   N/A   Available
 0/1   2      RTP   N/A   Available
 0/1   3      RTP   N/A   Available
 0/1   4      RTP   N/A   Available
 0/1   5      RTP   N/A   Available
 0/1   6      RTP   N/A   Available
 0/1   7      RTP   N/A   Available
 0/1   8      RTP   N/A   Available
 0/1   9      RTP   N/A   Available
 0/1   10     RTP   N/A   Available
 0/1   11     RTP   N/A   Available
 0/1   12     RTP   N/A   Available
 0/1   13     RTP   N/A   Available
```


show track

Use the **show track** command to display track object configuration and statistics. Refer to *Network Monitor Track Command Set on page 4098* for information on configuring track objects. Variations of this command include the following:

show track
show track <*name*>
show track <*name*> **realtime**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

> *Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<*name*>	Optional. Displays information only for the track object specified.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show track** command:

```
>enable
#show track track_1
Current State: PASS
    Dampening Interval: 30 seconds
    Test Value: probe_A (PASS) AND probe_B (FAIL)
    Track Changes: 3
    Time in current state: 25 days 2 hours, 34 minutes, 32 seconds
```

show udp info

Use the **show udp info** command to display User Datagram Protocol (UDP) session information. Variations of this command include:

show udp info
show udp info realtime
show udp info <*number*>
show udp info <*number*> **realtime**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

> *Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

<*number*>	Optional. Specifies ID of session to display. Valid range is **0** to **31**.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example shows sample output from the **show udp info** command:

>**enable**
#show udp info
UDP Session Entries

ID	Local Port	IP Address	Socket
2	520	0.0.0.0	1
3	0	0.0.0.0	4
4	161	0.0.0.0	5
5	8	127.0.0.1	7
6	10	0.0.0.0	11
7	6	127.0.0.1	16
8	4	127.0.0.1	17
9	14	127.0.0.1	18
10	12	127.0.0.1	19

show usbdrive0

Use the **show usbdrive0** command to display a list of all files currently stored in Universal Serial Bus (USB) flash drive memory. Variations of this command include:

show usbdrive0
show usbdrive0 *<filename>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<filename>	Optional. Displays details for a specified file located in USB flash drive memory. Enter a wildcard (such as ***.biz**) to display the details for all files matching the entered pattern.

Default Values

No default values are necessary for this command.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following is sample output from the **show usbdrive0** command:

```
>enable
#show usbdrive0
Files:
 245669 010100boot.biz
1141553 new.biz
    821 startup-config
   1638 startup-config.old
1175679 020016.biz
    821 startup-config.bak
2572304 bytes used, 4129776 available, 6702080 total
```


show usb attached-devices

Use the **show usb attached-devices** command to display statistics for universal serial bus (USB) devices attached to the USB wireless wide area network (WWAN) network interface module (NIM) or the USB port on the AOS unit. The output from this command includes the attached device identification, the product identification, the device class, the device manufacturer and model, and the slot and port used by the device. Variations of this command include:

show usb attached-devices

show usb attached-devices detail

The NetVanta USB WWAN NIM supports cellular connections through a USB cellular modem provided by the service provider. For more information about configuring the NetVanta USB WWAN NIM or the cellular interface, refer to Cellular Interface Command Set on page 2105 or the USB WWAN NIM and the Cellular Interface configuration guide available online at https://supportcommunity.adtran.com.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

detail	Displays all available device statistics.

Default Values

No default values are necessary for this command.

Command History

Release 17.8	Command was introduced.
Release 18.2	Command was expanded to include the **detail** parameter.

Functional Notes

The output of the **show usb attached-devices** commands is device-dependent, and some USB LTE modems may not respond with any output.

Usage Examples

The following is sample output from the **show usb attached-devices** command:

>**enable**
#show usb attached-devices
USB Device attached
VendorID: 1410
ProductID: 6000
DeviceClass: 0x2 (Communications)
Manufacturer: Novatel Wireless Inc.
Product: Novatel Wireless CDMA
Serial Number: 091138075581000
Slot/Port: 1/1
Number of Endpoints: 13
Endpoints: 1 INTERRUPT IN, 2 BULK IN, 2 BULK OUT, 4 BULK IN, 4 BULK OUT, 9 BULK IN, 9 BULK OUT, 10 BULK IN, 10 BULK OUT, 5 BULK IN, 6 BULK OUT, 7 BULK IN, 8 BULK OUT

The following is sample output from the **show usb attached-devices** command if an unknown device is attached to the 3G USB NIM:

>**enable**
#show usb attached-devices
USB Device attached
VendorID: 1457
ProductID: 1544
DeviceClass: 0x7 (Printer)
Manufacturer: Unknown
Product: Unknown
Serial Number: Unknown
Slot/Port: 1/1
Number of Endpoints: 0
Endpoints:

The following is sample output from the **show usb attached-devices** command if no USB device is attached to the 3G USB NIM:

>**enable**
#show usb attached-devices
No USB Device attached

show users

Use the **show users** command to display the name (if any) and state of users authenticated by the system. Variations of this command include:

show users
show users realtime

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

> *Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Displayed information includes:

- Connection location (for remote connections, this includes Transmission Control Protocol (TCP) information)
- User name of authenticated user
- Current state of the login (in process or logged in)
- Current enabled state
- Time the user has been idle on the connection

Usage Examples

The following is sample output from the **show users** command:

```
>enable
#show users
- CONSOLE 0 'adtran' logged in and enabled
 Idle for 00:00:00
- TELNET 0 (172.22.12.60:3998) 'password-only' logged in (not enabled)
 Idle for 00:00:14
- FTP (172.22.12.60:3999) 'adtran' logged in (not enabled)
 Idle for 00:00:03
```


show version

Use the **show version** command to display the current Adtran Operating System (AOS) version information.

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R12.1.0	Command output was modified for virtual AOS (vAOS) instances.

Functional Notes

In vAOS instances, the output of this command does not include checksum information, boot ROM or hardware versions, or boot system images names.

Usage Examples

The following is sample output from the **show version** command:

```
>enable
#show version

Adtran, Inc. OS version A5.01.00.E
  Mainline Version: M04
  Checksum: 894C9C39
  Built on: Fri Sep 09 11:31:09 2011
  Upgrade key: 29be9733e227e21d8f7d4af849dc7603
Hardware version C.1
Boot ROM version A3.01.00
  Checksum: 6A26
```


Built on: Wed Jul 08 16:52:15 2009
Copyright (c) 1999-2009, Adtran, Inc.
Platform: Netvanta 6334, part number 17006334G1, CLEI code is N/A
Serial number LBADTN0940AD077
Flash: 67108864 bytes DRAM: 134217727 bytes

show vlan

Use the **show vlan** command to display current virtual local area network (VLAN) information. Variations of this command include:

show vlan
show vlan brief
show vlan brief realtime
show vlan id <*vlan id*>
show vlan id <*vlan id*> **realtime**
show vlan name <*name*>
show vlan name <*name*> **realtime**
show vlan realtime

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

brief	Optional. Shows an abbreviated version of the VLAN information (brief description).
id <*vlan id*>	Optional. Shows information regarding a specific VLAN, specified by a VLAN interface ID (valid range: **1** to **4094**).
name <*name*>	Optional. Shows information regarding a specific VLAN, specified by a VLAN interface name (up to 32 characters).
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 10.1	The **realtime** display parameter was introduced.
Release 15.1	The **realtime** display parameter was added to **show vlan id** and **show vlan name**.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following is sample output from the **show vlan** command:

```
>enable
#show vlan
```

VLAN	Name	Status	Ports
- 1	Default	active	eth 0/5, eth 0/6, eth 0/8, eth 0/13, eth 0/14, eth 0/15, eth 0/16, eth 0/17, eth 0/18, eth 0/19, eth 0/20, eth 0/21, eth 0/22, eth 0/23, eth 0/24, giga-eth 0/1, giga-eth 0/2
2	accounting	active	eth 0/1, eth 0/2
3	VLAN0003	active	eth 0/3, eth 0/4, eth 0/7, eth 0/9, eth 0/10, eth 0/11, eth 0/12

VLAN	Type	MTU
- 1	enet	1500
2	enet	1500
3		

The following is an example of the **show vlan name** command that displays VLAN 2 (**accounting** VLAN) information:

```
>enable
#show vlan name accounting
VLAN              Name            Status      Ports
----------------- --------------- ----------- ---------------
- 2                accounting      active      eth 0/1, eth 0/2

VLAN              Type            MTU
----------------- --------------- -----------
- 2                enet            1500
```

show voice alias

Use the **show voice alias** command to display alias parameters. Aliases are used to mask identity settings, such as names and extensions. Variations of this command include:

show voice alias
show voice alias global
show voice alias group
show voice alias system
show voice alias user

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

global	Optional. Displays global aliases.
group	Optional. Displays group aliases.
system	Optional. Displays system aliases.
user	Optional. Displays user aliases.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows sample output from the **show voice alias** command:

```
>enable
#show voice alias

Alias           Translation     Type
--------------- --------------- ------------------
MyAlias         4433            Global

Total Displayed: 1
```


show voice available

Use the **show voice available** command to list foreign exchange station (FXS) ports that are not associated with a user.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays FXS ports that are not associated with a user:

```
>enable
#show voice available

Interface
-------------
fxs 0/1
fxs 0/2
```


show voice conference local

Use the **show voice conference local** command to view current conference sessions. Variations of this command include:

show voice conference local all
show voice conference local session <*number*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

all	Displays current status of all local conference sessions.
session <*number*>	Displays current status of the specified local conference session.

Default Values

No default values are necessary for this command.

Command History

Release A2	Command was introduced.

Usage Examples

The following example displays information about all local active conference sessions:

>enable
#show voice conference local all

ID	Originator (FXS)	Remote1	Remote2	RtpRsrc
1	2001 (0/1)	T01 (2565551234)	T02 (2568675309)	0/1.(1,2,3)
2	2004 (0/4)	2002 (FXS 0/2)	3001 (SIP)	0/2.(1,4,5)

The following example only displays information for local conference session 2:

>enable
#show voice conference local session 2

ID	Originator (FXS)	Remote1	Remote2	RtpRsrc
2	2004 (0/4)	2002 (FXS 0/2)	3001 (SIP)	0/2.(1,4,5)

show voice dial-plan

Use the **show voice dial-plan** command to view number display templates. Variations of this command include:

show voice dial-plan
show voice dial-plan *<number>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<number>	Optional. Displays information about a specific number display template.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays information about number display template **1**:

```
>enable
#show voice dial-plan 1
Type                    ID      Pattern
-------------------------------------------------------------------
Always Permitted        1       NXXNXXXXXX
```


show voice did

Use the **show voice did** command to display direct inward dialing (DID) information. Variations of this command include:

show voice did
show voice did groups
show voice did other
show voice did users

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

groups	Optional. Displays all DID entries for ring groups.
other	Optional. Displays all nonuser and nonring group DID entries.
users	Optional. Displays all DID entries for users.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays DID entries for ring groups:

```
>enable
#show voice did groups
```


show voice directory

Use the **show voice directory** command to display direct inward dialing (DID) information. Variations of this command include:

show voice directory
show voice directory *<name>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<name>	Optional. Specifies the name on the directory to display. Only extensions included in the specified directory will appear.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 14.1	Command was expanded.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all extensions sorted by extension number:

```
>enable
#show voice directory
Directory Name: SYSTEM
    User Name       External        Extension
    ------------------------------------------------------
    John Smith                      5006
    Jane Doe                        5005

    Directory Name: Engineering
    User Name       External        Extension
    ------------------------------------------------------
    John Doe        Yes             5551212
```


show voice door-phone

Use the **show voice door-phone** command to display the door phone account settings. A door phone is used to communicate with visitors prior to them entering an establishment.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows sample output from the **show voice door-phone** command:

```
>enable
#show voice door-phone

First     Last     Ext      Interface     Description
-------------------------------------------------------------------------------
Front     Door     4430     virtual       Front Door of Building
```


show voice extensions

Use the **show voice extensions** command to display all of the current voice extensions and their status.

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all extensions and the status of the extension:

```
>enable
#show voice extension

AccountID       Idle/Ring/Busy    Available   DND     FWD
-------------------------------------------------------------------------------
T01             Idle              *           -       -
T06             Idle              *           -       -
T02             Idle              *           -       -
5200            Idle              *           -       -
6000            Idle              *           -       -
6001            Idle              *           -       -
6002            Idle              *           -       -
6003            Idle              *           -       -
T03             Idle              *           -       -
2               Idle              *           -       -
1234            Idle              *           -       -
```


show voice grouped-trunk

Use the **show voice grouped-trunk** command to display all voice trunk groups.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all voice trunk groups:

```
>enable
#show voice grouped-trunk

Name        Resource-Selection      Description
-------------------------------------------------------------------------
SIP         linear                  SIP trunk
DSX         linear                  DSX trunk
DXS         linear                  DXS trunk
```


show voice line

Use the **show voice line** command to display voice line stations. Variations of this command include:

show voice line
show voice line <*station*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*station*>	Optional. Displays a specific voice line station name or extension on the system base on the valid **voice line** descriptors entered into the system.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows sample output from the **show voice line** command:

```
>enable
#show voice line
Line: 4444
Trunk: not configured
Registered Endpoints: 0
Call State: IDLE
Active Endpoints: N/A
DSP Resource: N/A

Line: Sales
Trunk: not configured
Registered Endpoints: 0
Call state: IDLE
--MORE--
```


show voice loopback calls

Use the **show voice loopback calls** command to display the status of the loopback call(s).

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A1	Command was introduced.

Usage Examples

The following example displays all voice loopback calls:

```
>enable
#show voice loopback calls
ID   Extension    Codec  Status                          Number          Duration (hour:min:sec)
-------------------------------------------------------------------------------------------------------------------------
 1   1123                <ENDED (invalid number)    -> 8837655          :01
 2   1123                 Calling                   -> 4001             :05
 3   1123                <ENDED (no appearances)    <- 4001             :01
 4   1123          G729   Connected                 -> 4001             :07
```


show voice mail

Use the **show voice mail** command to display voice mail information for the system or a specific user. Variations of this command include:

show voice mail
show voice mail <*number*>
show voice mail notify-schedule <*number*>

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*number*>	Optional. Displays voice mail information for the specified user's extension.
notify-schedule <*number*>	Optional. Displays the voice mail notification schedule for the specified user's extension.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows sample output from the **show voice mail** command:

```
>enable
#show voice mail
                                    New   Num   Total Time   Total Time   Greeting
AccountID  VM COS                   Msg   Msg   Used        Free         Time
-------------------------------------------------------------------------------------------------------------------
1000                                -     -     00:00:00    00:00:00     00:00
2000                                -     -     00:00:00    00:00:00     00:00
2001       normal_voicemail         38    38    00:09:54    00:00:06     00:02
2002       normal_voicemail         40    40    00:09:49    00:00:11     00:02
2003       normal_voicemail         39    39    00:09:54    00:00:06     00:02
2004       normal_voicemail         35    35    00:09:55    00:00:05     00:01
```


2005	normal_voicemail	20	20	00:09:28	00:00:32	00:01
2006	normal_voicemail	41	41	00:09:54	00:00:06	00:02
2015	normal_voicemail	42	42	00:09:57	00:00:03	00:01
2016	executive_voi...	74	74	00:18:11	00:11:49	00:02
2017	executive_voi...	75	75	00:11:03	00:18:57	00:01
2018	normal_voicemail	34	34	00:09:38	00:00:22	00:01
2019	normal_voicemail	35	35	00:09:42	00:00:18	00:01
2020	executive_voi...	73	73	00:20:41	00:09:19	00:01
0		-	-	00:00:00	00:00:00	00:00

The following is sample output for the **show voice mail** <*number*> command for extension **2017**:

```
>enable
#show voice mail 2017

Voicemail information for account:?:5T
 VM Class of Service:     executive_voicemail
 Standard Greeting:       00:09          Total Voicemail Usage:   00:11:04
 Alternate Greeting:      00:10          Total Voicemail Free:    00:18:56
 Recorded Name:           00:01

Message 1 of 75
 Time/Date: 00:28:16 CST Sun Feb 07 2106
 Calling Party: UNKNOWN (UNKNOWN)
 Length: 00:00
 Status: Old
```

The following is sample output for the **show voice mail notify-schedule** <*number*> command for extension **2017**:

```
>enable
#show voice mail notify-schedule 2017

Start                End                  Email1        Email2
-------------------------------------------------------------------------------------
Sun 12:00 am         Mon 7:59 am          ----          ----
Mon 8:00 am          Thu 11:59 pm         Yes           ----
Fri 12:00 am         Sat 11:59 pm         ----          ----
```


show voice match

Use the **show voice match** command to display voice automatic number identification (ANI) substitution parameters. Variations of this command include:

show voice match
show voice match ani <*template*>

> 
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

match	Displays all substitution configurations.
ani <*template*>	Optional. Displays a specific ANI substitution entry.

Default Values

No default values are necessary for this command.

Command History

Release A2	Command was introduced.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits

5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example displays voice substitution information:

>**enable**
#show voice match

ani - match: 2323
substitute: 5555

show voice music-on-hold statistics

Use the **show voice music-on-hold statistics** command to display music on hold player statistics.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example displays music on hold player statistics:

```
>enable
#show voice music-on-hold statistics

MOH Player      Codec       IpAddress       Port
System          PCMU        10.17.20.38     3002        default player

MOH Player      NumRegApps  Codec           Play Status File Name
System          1           PCMU            Playing     welcome.wav

#
```


show voice named-digit-timeouts

Use the **show voice named-digit-timeouts** command to view configured named digit timeouts (NDTs) and their values. The output for this command includes the default NDT value. Variations of this command include:

show voice named-digit-timeouts
show voice named-digit-timeouts <*name*>

> NOTE
>
> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*name*>	Optional. Displays information about a specific named digit timeout.

Default Values

No default values are necessary for this command.

Command History

Release A2	Command was introduced.

Usage Examples

The following example displays all named digit timeouts and their timeout value:

```
>enable
#show voice named-digit-timeouts
Name                    Timeout Value (secs)
------------------------------------------------------------------------------
default                 4
long                    10
longer                  12
longest                 16
short                   6
shorter                 5
shortest                2
```


show voice operator-group

Use the **show voice operator-group** command to display all operator groups.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all operator groups:

```
>enable
#show voice operator-group
Operator-group: 0      Call distribution type: all
Number of calls allowed: 1
Number of rings before coverage: 4

Extension  Firstname            Lastname        Logged In
-------------------------------------------------------------------------------
2001           John                 Smith              *

Order       # of Rings      Call Coverage Action
-------------------------------------------------------------------
1                0              Auto Attendant
2                2                  None
3                2                  None
4                2                  None
5                2                  None
```


show voice phone-files

Use the **show voice phone-files** command to display files required for Session Initiation Protocol (SIP) phone configuration.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows sample output from the **show voice phone-files** command:

```
>enable
#show voice phone-files

03/02/2006 16:03 PM          216 0004f203f69c.cfg
03/02/2006 16:03 PM          687 5001-0004f203f69c.cfg
03/02/2006 16:03 PM          216 0004f203b0d6.cfg
03/14/2006 16:03 PM          306 polycom.cfg
7 File(s)          132516 bytes
0 Dir(s)           0 bytes
21019575 bytes used, 9720360 available, 30739935 total
```


show voice pickup-group

Use the **show voice pickup-group** command to display all configured call pickup groups (or a specific group). Variations of this command include:

show voice pickup-group

show voice pickup-group *<name>*

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<name>	Optional. Specifies a particular call pickup group to display.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following is sample output from the **show voice pickup-group** command:

```
(config)#show voice pickup-group
        Pickup Group: Group1
        Description: 4th floor sales
        Pickup Group Extension: 8508

        Members    Firstname      Lastname
        ---------------------------------------------
        0330          Vickie       Spinaker
        2003          Marc          Starkalous
        2013          Patrick       Wales
        2007          Drew          Lever
        2006          Sarah         Williams
        1012          Jessica       Thomas
```


show voice quality-stats

Use the **show voice quality-stats** command to display voice quality statistical information. Variations of this command include the following:

show voice quality-stats
show voice quality-stats active
show voice quality-stats active realtime
show voice quality-stats <*id*>
show voice quality-stats <*id*> **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*Using the **realtime** argument for this command can adversely affect the performance of your unit.*

Syntax Description

active	Displays all quality statistics for active calls.
<*id*>	Specifies an identity number of a call to obtain detailed statistics.
realtime	Optional. Displays full-screen output in real time. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example displays voice quality statistics for all active calls:

>**enable**
#show voice quality-stats active

ID	Start Time	From	To	Duration	Codec	Lost Pkts	Discard Pkts	Delay Avg	Delay Max
4236	3:02 pm	5152222	5157744	6:55	G711	2	0	50	50

show voice queue

Use the **show voice queue** command to display the status of the call queuing feature. Variations of this command include:

show voice queue
show voice queue <*extension*>
show voice queue detail
show voice queue detail <*extension*>

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*extension*>	Optional. Specifies the extension of the call queue to display.
detail	Optional. Displays detailed call queue information.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example displays status information for the call queue at extension **6407**:

```
>enable
#show voice queue 6407
Call Queue: 6407        Call distribution type: ring-all
Name: TSqueue
Description: Tech Support Call Queue

Max allowed number of queued calls: 16
Operation: active
State: unlocked

Current queue stats:
        Calls: 1
        Longest Wait: 30
```


24 Hour Stats:

calls queued: 87

calls Abandoned: 1 calls overflowed:

longest wait time: 30 average wait time: 13

Members	Firstname	Lastname	Logged In
2013	Patrick	Wales	*
2004	John	Taylor	*
2003	Marc	Starkalous	*#

show voice ring-group

Use the **show voice ring-group** command to display all ring groups. Variations of this command include:

show voice ring-group
show voice ring-group <*number*>

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<*number*>	Optional. Displays information about a specific ring group extension.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all ring groups:

```
>enable
#show voice ring-group
ring-group   1234          type: linear
description:
Number of calls allowed: 1
First        Last          Ext          Logged In
-------------------------------------------------------------------------
Order        NumRings      Action
-------------------------------------------------------------------------
1            2             None
2            2             None
3            2             None
4            2             None
5            2             None
```


ring-group 2 type: linear
description:
Number of calls allowed: 1

First	Last	Ext	Logged In

Order	NumRings	Action
1	2	None
2	2	None
3	2	None

show voice speed-dial

Use the **show voice speed-dial** command to display system speed dial information. Variations of this command include:

show voice speed-dial
show voice speed-dial <*number*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*number*>	Optional. Displays information about a specific speed dial number. Valid range is **1** to **99**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays information on speed dial number **50**:

```
>enable
#show voice speed-dial 50
speed-dial - ID: 50
    Name: Main Office
    Number: 4000
```


show voice spre

Use the **show voice spre** command to display all special prefix (SPRE) code mappings. Functions with no SPRE code assigned are not displayed. Variations of this command include:

show voice spre local
show voice spre network

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

local	Displays all SPRE codes used locally.
network	Displays all SPRE codes passed through to the network.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release A1.02	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all local SPRE codes:

```
>enable
#show voice spre local

Current SPRE Handling Mode:  Local

SPRE Code                    Description
-------------------------------------------------------------------------------------------------------
**                           Hands Free Auto-Answer

*20n                         System Mode 0=Deflt, 1=Night, 2=Lunch, 3=Wknd, 7=Override
*21xxxx                      Billing Code
*25nn                        System Speed Dial
```


*30	Page-Overhead
*31x	Page intercom (0=all, 1-9=zone)
*32	Forward Notification Cancel
*33xxxx	Call Forward + Extension
*34xxxx*pppp*nxxxxxx	Call Forward Remote
*35	Call Forward Cancel
*36xxxx*pppp*	Remote Call Forward Cancel
*37	Door Phone
*38	Door Unlock
*39x	Do Not Disturb Enable/Disable
*44	Permanent Hold
*46xxxx*pppp*	Hotel Login
47pppp	Hotel Logout
52xxxx	Pickup Extension
55xxxx	Group Login
56xxxx	Group Logout
57pppp	User Station/Phone Lock
58pppp	User Station Unlock
*61nnxxxx	Program User Speed Dial
*62nn	Call User Speed Dial
*63xxxx*pppp*	MACA Login
64pppp	MACA Logout
*65	Cancel Camp-on
*66	Camp on a Busy Extension
*67	Block Call-ID delivery for this call only
*69	Call Return
*70	Disable Call Waiting on a per call basis
*72	Call last dialed number
74xxxx	CallQueue Login
76xxxx	CallQueue Logout
*77z	Call Park + Zone
*78z	Call Park Retrieve
79[pw-old][pw-new]*	Set Account Password
*86xxxx	Send User Directly to Voicemail
*88	Transfer
*90xxxx	Class of Service Override (xxxx=Override Passcode)
*95xxxx	Set Message Waiting
*96xxxx	Clear Message Waiting
*97x	Auto-Answer Do Not Disturb
*98	Voicemail

show voice status-group

Use the **show voice status-group** command to display information on all voice status groups or on a specified group. Variations of this command include:

show voice status-group
show voice status-group *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<name>	Optional. Displays all users within the specified status group.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all voice status group extensions:

>enable
#show voice status-group

Status-group: Sales Team
Description:

Type	Member ID	Display Name	Status
user	2001	Martha	Idle
user	3002	Dan	Idle
user	3003	Betty	Idle
user	3004	Chris	Idle
user	4001	Jami	Idle

Number of members: 5

show voice switchboard

Use the **show voice switchboard** command to display all voice switchboard extensions.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example displays all voice switchboard extensions:

```
>enable
#show voice switchboard
Ext
----
1234
2
5200
6000
6001
6002
6003
```


show voice system-mode

Use the **show voice system-mode** command to display the current system mode running on the unit. Specifying a day will display any transitions configured for that day. Variations of this command include:

show voice system-mode
show voice system-mode sunday
show voice system-mode monday
show voice system-mode tuesday
show voice system-mode wednesday
show voice system-mode thursday
show voice system-mode friday
show voice system-mode saturday

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

[sunday - saturday]	Optional. Displays the specified system mode programmed in the unit. Choose from Sunday through Saturday.

Default Values

No default values are valid for this command.

Command History

Release A1	Command was introduced.

Usage Examples

The following example shows sample output from the **show voice system-mode monday** command:

```
>enable
#show voice system-mode monday
Current system-mode: default
System-mode transition - Day: monday
        Mode @ time: lunch @ 12:00
        Mode @ time: default @ 13:00
        Mode @ time: night @ 17:00
```


The following is sample output from the **show voice system-mode** command:

>**enable**
#show voice system-mode
Current system-mode: weekend

show voice trunk

Use the **show voice trunk** command to display all voice trunks. Variations of this command include:

show voice trunk
show voice trunk *<trunk id>*
show voice trunk connects *<trunk id>*
show voice trunk server-cache

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

connects	Optional. Displays all trunk voice interface connections.
<trunk id>	Optional. Displays voice trunk information for a specific trunk ID. Use T01, T02, and so on for the trunk ID.
server-cache	Optional. Displays information contained in the voice trunk Session Initiation Protocol (SIP) server cache.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release R13.8.0	Command was expanded to include the **server-cache** parameter.

Usage Examples

The following example displays all voice trunks:

```
>enable
#show voice trunk
```

Trunk Name	Resource Selection	Busy Admin. Config.	Busy Admin. Status	Busy Attempts Today	Non Busy Attempts Today	Busy Attempts Total	Non Busy Attempts Total
T01	linear	Not Busy	Not Busy	0	0	0	7
T06	linear	Not Busy	No Connects	0	0	0	0
T02	linear	Not Busy	Not Busy	0	0	0	27
T03	linear	Not Busy	No Connects	0	0	0	0

show voice trunk monitor

Use the **show voice trunk monitor** command to display the configuration settings for Session Initiation Protocol (SIP) trunks used for SIP trunk failover on the AOS system. Displayed settings include any trunks configured with SIP trunk failover, any configured recovery delay, and the address, port, and status of any failover servers.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example displays the configuration information for SIP trunks used in a failover situation:

```
>enable
#show voice trunk monitor
Trunk:                                  T01
Delay                                   Min 3600
Servers:
    Address                                 | Port    | Status
    111.111.111.111                         | 5060    | Up *
    222.222.222.222                         | 5060    | Down
    2001:0DB8:AC10:FE01:0000:0000:0000:0000 | 12345   | Delay   Remaining 97 s
```


show voice users

Use the **show voice users** command to display all voice user stations. Variations of this command include:

show voice users
show voice users did
show voice users extension
show voice users last
show voice users location

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

did	Optional. Displays all users included in the directory.
extension	Optional. Displays directory entries sorted by extensions.
last	Optional. Displays directory entries sorted by last name.
location	Optional. Displays the location of users in the directory.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 14.1	Command was expanded.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.03	Command was expanded to include the **location** parameter.

Usage Examples

The following example displays all voice users:

```
>enable
#show voice users
First       Last        Ext         Interface Description
----------------------------------------------------------------------------
Janet       Smith       5200        virtual
Bill        Jones       6000        virtual
Sam         Sampson     6001        virtual
```


show voice users sip

Use the **show voice users sip** command to display a list of Session Initiation Protocol (SIP) users with their associated ports.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following is sample output from the **show voice users sip** command:

```
>enable
#show voice users sip

First          Last         Extension      Interface MAC Address      IP Address
-------------------------------------------------------------------------------------------------------------------
Fronia         Cobins       4430           Unregistered user - Unable to resolve port
Gorge          Owens        4440           Unregistered user - Unable to resolve port
Heather        Virginia     4450           Unregistered user - Unable to resolve port

Total number of configured SIP voice users: 3
```


show voip name-service cache

Use the **show voip name-service cache** command to view Voice over Internet Protocol (VoIP) name service information stored in the cache.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A2.04	Command was introduced.

Functional Notes

The information displayed in the show command output consists of two columns. The left column lists the host name of an entry in the VoIP Name Service Name Table. This corresponds with the entries shown in the output of the command *show voip name-service name-table on page 1109*. The right column shows the corresponding last resolved IP address(es) of the entry. An IP address of all zeros indicates the particular host has not been resolved. In the event all domain naming system (DNS) servers are unreachable and a particular host name cannot be refreshed, the DNS uses the cached address to resolve the particular host.

Usage Examples

The following example displays name service information stored in the cache:

```
>enable
#show voip name-service cache

Name                                    Last Resolved Address
-------------------------------------------------------------------------------------------
test2.pprice.voice.test.adtran.com      1.2.3.3
bogus3.pprice.voice.test.adtran.com     1.2.3.3
test.pprice.voice.test.adtran.com       0.0.0.0
bogus1.pprice.voice.test.adtran.com     1.2.3.1
bogus2.pprice.voice.test.adtran.com     1.2.3.2
```


show voip name-service name-table

Use the **show voip name-service name-table** command to view Voice over Internet Protocol (VoIP) name service information in the name table.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A2	Command was introduced.

Functional Notes

The following information is displayed in the show command output:

- **Name** - Indicates the name of the service.
- **Proto** - Indicates the protocol.
- **Tpt** - Indicates the transport method used, either User Datagram Protocol (UDP) or Transmission Control Protocol (TCP).
- **LastSrc** - Indicates the last software object that requested this domain naming system (DNS) entry be cached. Valid options are **trunk**, **route**, **manual**, **proxy**, **MGCP**, or **derived**.
- **Interval** - Indicates when the entry will expire.
- **Users** - Indicates the number of software objects using this entry.
- **Resolved** - Indicates whether or not the DNS has been able to resolve this entry.

Usage Examples

The following example displays name service information in the name table:

```
>enable
#show voip name-service name-table
```

Name	Proto	Tpt	LastSrc	Interval	Users	Resolved
pq.adtran.com	SIP	UDP	trunk	0h 59m 47s	2	Yes
bw2.pq.adtran.com	SIP	UDP	trunk	0h 59m 46s	2	Yes

Technology Review

VoIP name service maintains a list of service names relevant to VoIP transactions while also facilitating access between VoIP-related queries to the external DNS server and the internal DNS client. Service names are automatically entered and deleted from the internal service name table when configured or not configured for VoIP-related subsystems. The VoIP name service begins polling external DNS servers for recently added service names to preemptively resolve service names before they are deleted. Using the **show voip name-service name-table** command will show the status of added service names.

show voipwizard log

Use the **show voipwizard log** command to display the log file from the Voice over IP (VoIP) Setup Wizard.

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.3.0	Command was introduced.

Usage Examples

The following example displays the VoIP Setup Wizard log file:

```
>enable
#show voipwizard log
VCID: 1 (NV1638)
Using 19358 bytes

********** SUMMARY *************
Ports successfully assigned as voice ports: (switchport 0/1-24)
Ports successfully assigned as uplink ports: (gigabit-switchport 0/1-4)

Voice port configuration: description voice
                          spanning-tree edgeport
                          no shutdown
                          switchport voice vlan 2
                          qos trust cos
Uplink port configuration: description uplink
                           no shutdown
                           switchport mode trunk
                           qos trust cos

--MORE--
```


show vrf

Use the **show vrf** command to display the configured virtual routing and forwardings (VRFs) and the interfaces associated with each one (or a specific VRF). Variations of this command include:

show vrf
show vrf *<name>*
show vrf interfaces
show vrf interfaces *<name>*

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

*To view secondary IP addresses, use the **show running-config** command.*

Syntax Description

<name>	Optional. Displays information for only the specified VRF.
interfaces	Optional. Displays information about interfaces associated with all configured VRFs.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **show vrf** command:

```
>enable
#show vrf
Name            Default RD      Interfaces
-Default-       0:0             eth 0/1
                                ppp 1
Engineering     100:1           vlan 11
                                vlan 12
Accounting      100:2           vlan 21
                                vlan 22
```

The following is sample output from the **show vrf interfaces** command:

```
>enable
#show vrf interfaces
Interface       IP Address      VRF             Protocol
eth 0/1         10.0.0.1                        DOWN
ppp 1           10.0.1.1                        UP
vlan 11         1.1.1.1         Engineering     UP
vlan 12         1.1.2.1         Engineering     UP
vlan 21         2.1.1.1         Accounting      UP
```

show vrrp

Use the **show vrrp** command to display configuration and operating data for Virtual Router Redundancy Protocol (VRRP) configurations. Variations of this command include:

show vrrp
show vrrp brief
show vrrp interface <*interface*>
show vrrp interface <*interface*> **group** <*number*>
show vrrp statistics
show vrrp statistics interface <*interface*>
show vrrp statistics interface <*interface*> **group** <*number*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

brief	Optional. Limits the amount of data shown.
group <*number*>	Optional. Displays data or statistics for a specified VRRP group on the specified interface. Group numbers range from **1** to **255**.
interface <*interface*>	Optional. Displays data or statistics for all VRRP groups or a specified group on the specified interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network (VLAN) interface, use **vlan 1**. Type **show vrrp interface ?** for a complete list of valid interfaces.
statistics	Optional. Displays statistics for all VRRP groups on all interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface and the gigabit switchport interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

Although VRRP group virtual router identifiers (VRIDs) can be numbered between 1 and 255, only two VRRP routers per interface are supported.

Usage Examples

The following example gives sample output from the **show vrrp statistics** command:

```
eth 0/1
Group 1
    Became Master: 3
    Priority Zero Packets Sent: 1
    Priority Zero Packets Received: 0
    Advertisements Sent: 105134
    Advertisements Received: 241
        Advertisements Interval Errors: 0
        Advertisements TTL Errors: 0
        Advertisements Address List Errors: 0
        Advertisements Packet Length Errors: 0
Group 2
    Became Master: 1
    Priority Zero Packets Sent: 0
    Priority Zero Packets Received: 0
    Advertisements Sent: 897
    Advertisements Received: 1628
        Advertisements Interval Errors: 0
        Advertisements TTL Errors: 0
        Advertisements Address List Errors: 0
        Advertisements Packet Length Errors: 0
```

show vrrpv3

Use the **show vrrpv3** command to display configuration and operating data for Virtual Router Redundancy Protocol version 3 (VRRPv3) configurations. Variations of this command include:

show vrrpv3
show vrrpv3 brief
show vrrpv3 interface <*interface*>
show vrrpv3 interface <*interface*> **group** <*vrid*>
show vrrpv3 interface <*interface*> **group** <*vrid*> **ipv4**
show vrrpv3 interface <*interface*> **group** <*vrid*> **ipv6**
show vrrpv3 statistics
show vrrpv3 statistics interface <*interface*>
show vrrpv3 statistics interface <*interface*> **group** <*vrid*>
show vrrpv3 statistics interface <*interface*> **group** <*vrid*> **ipv4**
show vrrpv3 statistics interface <*interface*> **group** <*vrid*> **ipv6**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

brief	Optional. Limits the amount of data displayed.
interface <*interface*>	Optional. Displays data or statistics for all VRRPv3 groups or a specified group on the specified interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network (VLAN) interface, use **vlan 1**. Type **show vrrp interface ?** for a complete list of valid interfaces.
group <*vrid*>	Optional. Displays data or statistics for a specified VRRPv3 group virtual router IDs (VRIDs) on the specified interface. Group VRIDs range from **1** to **255**.
ipv4	Optional. Displays data or statistics for the VRRPv3 group's IPv4 address family.
ipv6	Optional. Displays data or statistics for the VRRPv3 group's IPv6 address family.
statistics	Optional. Displays statistics for all VRRPv3 groups on all interfaces.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.
Release R10.11.0	Command was expanded to include the **ipv4** and **ipv6** parameters.

Functional Notes

Although VRRPv3 group VRIDs can be numbered between 1 and 255, only two VRRPv3 routers per interface per IP version are supported.

Usage Examples

The following example gives sample output from the **show vrrpv3** command:

```
>enable
#show vrrpv3
eth 0/1
  Group 1 - Address-Family IPv6
    State: Master
    Administrative state: UP
    Description:
    Configured Priority: 100, Actual Priority: 100
    Number of Addresses: 1
    Virtual Link-Local Address: FE80::7890
    Virtual Global Address: 00:00:5E:00:02:01
    Virtual MAC Address: 00:00:5E:00:02:01
    Accept-Mode is enabled
    Advertisement interval: 1 second(s)
    Preemption: Enabled - delay 0 second(s)
    Last Transition: 0:00:00:02
    Master Router Address: FE80::2A0:C8FF:FE23:21E0 (local) Priority: 100
```

show vxlan

Use the **show vxlan** command to display information regarding virtual extensible local area network (VxLAN) configuration on your AOS product. Variations of this command include:

show vxlan host
show vxlan host tunnel <*interface id*>
show vxlan host vni <*number*>
show vxlan peers
show vxlan peers tunnel <*interface id*>
show vxlan vni
show vxlan vni tunnel <*interface id*>

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

host	Displays information, sorted by tunnel ID, for active VxLAN tunnels on this device.
host tunnel <*interface id*>	Optional. Displays VxLAN information for the specified tunnel interface. Valid tunnel range is **1** to **1024**.
host vni <*number*>	Optional. Displays VxLAN information for the specified VNI. Valid VNI range is **1** to **677215**.
peers	Displays information, sorted by tunnel ID, for all VxLAN peers connected to this device.
peers tunnel <*interface id*>	Optional. Displays information for the VxLAN peer connected to the specified tunnel interface. Valid tunnel range is **1** to **1024**.
vni	Displays information, sorted by VNI, for all active VxLAN tunnels.
vni tunnel <*interface id*>	Optional. Displays VxLAN information, sorted by VNI, for the specified tunnel interface.Valid VNI range is **1** to **1024**.

Default Values

No default values are necessary for this command.

Command History

Release 13.1.0	Command was introduced.

Usage Examples

The following is sample output from the **show vxlan** command:

```
>enable
#show vxlan host vni 100
DestnationMac       TunnelId    VniId    DestinationVtep    Type          TTL(Sec)

00:11:22:33:44:AD   1           100      10.0.2.15          DYNAMIC       1477

>enable
#show vxlan peers
Tunnel ID       Source IP       Destination IP       Dest port       MTU
 1              10.0.2.17       10.0.2.15            4789            1464

>enable
#show vxlan vni tunnel 1
Source interface    Vlan-id    VNI        Tunnel
eth 0/2.1           2          100        tunnel 1
```

sip check-sync

Use the **sip check-sync** command to send a check-sync notification to all IP phones registered to the unit. When an IP phone receives this check-sync notification, the phone will check for possible configuration changes stored on the server. Variations of this command include the following:

sip check-sync
sip check-sync firmware-upgrade
sip check-sync *<user name or ip address>*

Syntax Description

firmware-upgrade	Optional. Specifies a check-sync to be used when upgrading phone firmware.
<user name or ip address>	Optional. Specifies the phone to contact with configuration changes.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example notifies all IP phones to check for a change in configuration:

>**enable**
#sip check-sync

ssh <*url*>

Use the **ssh** <*url*> command to create a secure shell (SSH) client connection between the AOS unit and another device. Variations of this command include:

ssh <*url*>
ssh <*url*>**myprivkey**
ssh <*url*>**myprivkey** <private key for SSH authentication>
ssh <*url*> **myprivkey dsa**
ssh <*url*> **myprivkey ecdsa256**
ssh <*url*> **myprivkey ecdsa384**
ssh <*url*> **myprivkey ecdsa512**
ssh <*url*> **myprivkey rsa**
ssh <*url*> **myprivkey rsa-sha2-512**
ssh <url> **port** <*port*>
ssh <*url*> **port** <port number> **myprivkey** <private key for SSH authentication>
ssh <*url*> **port** <port number> **myprivkey dsa**
ssh <*url*> **port** <port number> **myprivkey ecdsa256**
ssh <*url*> **port** <port number> **myprivkey ecdsa384**
ssh <*url*> **port** <port number> **myprivkey ecdsa512**
ssh <*url*> **port** <port number> **myprivkey rsa**
ssh <*url*> **port** <port number> **myprivkey rsa-sha2-512**
ssh <*url*> **privkey** <*filename of private key file*>
ssh <*url*> **source-interface** <*interface*>
ssh <*url*> **source-interface bvi** <*bridged virtual interface number*>
ssh <*url*> **source-interface gigabit-interface** <*gigabit interface slot/port*>
ssh <*url*> **source-interface loopback** <*loopback interface number: 1-1024*>
ssh <*url*> **source-interface ppp** <*PPP interface number*>
ssh <*url*> **source-interface tunnel** <*Tunnel interface number: 1-1024*>

Syntax Description

<*url*>	Specifies the uniform resource locator (URL) of the far end device. The format of the URL string must be **user@**<***ip address*** | ***hostname***>, for example, **MGARCIA@10.10.10.1** or **MGARCIA@domain.com**. IPv4 and IPv6 addresses as well as hostnames are supported in the URL definition. Optionally, you may include a password for the SSH connection using the format **user:password@**<***ip address*** | ***hostname***>, for example, **MGARCIA:password@10.10.10.1**.
myprivkey	Optional: This is a private key for SSH authentication. Available solutions are: **dsa**, **ecdsa256**, **ecdsa384**, **ecdsa521**, **rsa**, and **rsa-sha2-512**.
privkey	Optional. Filename of the private key file (PEM format).

port <*port*>	Optional. Specifies a port to use for connecting with the remote device instead of the default SSH port 22. Valid range is **1** to **65535**. Interface is optional. Valid values are: **myprivkey**, **privkey** and **source-interface**.
source-interface <*interface*>	Optional. Specifies the interface to be used as the source IP address for the SSH connection. Specify an interface in the format <*interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **ssh** <*url*> **source-interface** for a complete list of valid interfaces. Options are: Bridged virtual interface <*BVI number*> gigabit-ethernet <*slot/port*> loopback interface number <*1-1024*> tunnel interface <*1-1024*>

Default Values

When SSH client connections are created, by default they use port **22** and the default VRF.

Command History

Release R12.2.0	Command was introduced.
Release R14.4.0	Command was expanded to include myprivkey dsa, rsa, rsa-sha2-512, ecdsa256, ecdsa384, and ecdsa521 parameters.

Functional Notes

If you do not specify a password when using this command, you will be prompted for a password from the far end machine after entering the command.

Usage Examples

The following example creates an SSH client connection for the user **MGARCIA** on a target host of **10.10.10.1**, using the default SSH port:

```
>enable
#ssh MGARCIA@10.10.10.1
```

The following example creates an SSH client connection for the user **MGARCIA** on a target host of **10.10.10.1**, using **myprivkey** with source-interface **dsa.**

```
>enable
#ssh MGARCIA@10.10.10.1 myprivkey dsa
```


ssh key regenerate

Use the **ssh key regenerate** command to generate a new digital signature algorithm (DSA) or Rivest-Shamir-Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) key pair for SSH connections. When a new key file is generated, it erases the old key file. Variations of this command include:

ssh key regenerate
ssh key regenerate <*key*>
ssh key regenerate dsa
ssh key regenerate ecdsa
ssh key regenerate ecdsa <*key length*>
ssh key regenerate ecdsa 256
ssh key regenerate ecdsa 384
ssh key regenerate ecdsa 521
ssh key regenerate rsa <*key length*>
ssh key regenerate rsa 2048
ssh key regenerate rsa 3072
ssh key regenerate rsa 4096
ssh key regenerate sftp <*key*>
ssh key regenerate sftp dsa
ssh key regenerate sftp ecdsa <*key length*>
ssh key regenerate sftp ecdsa 256
ssh key regenerate sftp ecdsa 384
ssh key regenerate sftp ecdsa 521
ssh key regenerate sftp rsa <*key length*>
ssh key regenerate sftp rsa 2048
ssh key regenerate sftp sa 3072
ssh key regenerate sftp rsa 4096

Syntax Description

dsa	Optional. Limits the generation to only SFTP DSA keys.
ecdsa <*input*>	Optional. Limits the generation to only SFTP ECDSA keys. Supported ECDSA Key length are: 256, 384 and 521.
rsa <*input*>	Optional. Limits the generation to only RSA keys. Supported Key lengths are: 2048, 3072 and 4096.
sftp <*input*>	Optional. Limits the generation to only SFTP, DSA, RSA, and ECDSA key types.
dsa <*key length*>	Optional. Limits the generation to only SFTP DSA keys.
ecdsa <*key length*>	Optional. Limits the generation to only SFTP ECDSA keys. Supported key lengths are 256, 384. and 521.
rsa <*key length*>	Optional. Limits the generation to only SFTP RSA keys. Supported key lengths are 2048, 3072 and 4096.

Default Values

By default, a key file is generated when the system boots for the first time.

Command History

Release 10.10.0	Command was introduced.
Release R12.2.0	Command was expanded to include the **dsa** and **rsa** parameters, as well as support for RSA keys.
Release 13.11.0	Command was expanded to include the **sftp**, **sftp dsa,** and **sftp rsa** parameters, as well as support for SFTP keys.
Release 14.3.0	Command was expanded to include **rsa** (3072 and 4096), **ecdsa** (256, 384 and 521) keys for SSH and SFTP connections.

Functional Notes

When the **ssh key regenerate** command is entered without the optional **dsa**, **rsa,** or **sftp** keywords, by default, all key types are regenerated.

Usage Examples

The following example generates a new **dsa** key file for SSH connections:

>enable
#ssh key regenerate dsa

The following example generates a new **ecdsa** with a key length of **256**:
>enable
#ssh key regenerate ecdsa 256

The following example generates a new **sftp** for **rsa** with a key length of **4096.**
>enable
#ssh key regenerate sftp rsa 4096

ssh port-forward

Use the **ssh port-forward** command to create a secure shell (SSH) tunnel between the AOS unit and another device. Variations of this command include:

ssh port-forward <*port-forward port*> <*url*>
ssh port-forward <*port-forward port*> <*url*> **myprivkey dsa**
ssh port-forward <*port-forward port*> <*url*> **password** <*password*>
ssh port-forward <*port-forward port*> <*url*> **port** <*port*>
ssh port-forward <*port-forward port*> <*url*> **port** <*port*> **myprivkey dsa**
ssh port-forward <*port-forward port*> <*url*> **port** <*port*> **password** <*password*>
ssh port-forward <*port-forward port*> <*url*> **port** <*port*> **privkey** <*filename*>
ssh port-forward <*port-forward port*> <*url*> **privkey** <*filename*>

The maximum number of simultaneous port forward sessions is 10. However, this number could be reduced if there are not enough TCP resources due to other applications using them.

Syntax Description

<*port-forward port*>	Specifies the forwarded port on the local unit.
<*url*>	Specifies the uniform resource locator (URL) of the far end listening address. The format of the URL string must be **user@server:remote-port**, for example, MGARCIA@10.10.10.1:7000. Optionally, you may include the IP address of an interface on the remote machine using the format **user@server:remote-port:FarEndListenAddress**, for example, MGARCIA@10.10.10.1:7000:10.10.10.2. If a far end listen address is not included as part of the URL, localhost is assumed, and only those users logged into the remote machine can use the tunnel.
myprivkey dsa	Optional. Specifies to use the AOS unit's digital signature algorithm (DSA) private key for SSH authentication.
password <*password*>	Optional. Specifies a password to use for SSH authentication.
port <*port*>	Optional. Specifies a port to use for the underlying SSH protocol instead of the default SSH port 22. Valid range is **1** to **65535**.
privkey <*filename*>	Optional. Specifies a private key file to use for SSH authentication.

Default Values

No default values are necessary for this command.

Command History

Release 11.4.0	Command was introduced.

Functional Notes

Port forwarding via SSH is a technology that uses a secure tunnel between a local computer and a remote computer in order to relay data from other services. Because the tunnel is secure, it can be used to forward data from services that are inherently insecure. Port forwards on AOS devices support the following applications: Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), SSH, and Telnet.

To use this feature, your network must allow encrypted outbound sessions to be created through your firewall. Most firewalls allow encrypted outbound sessions by default.

If you do not specify a password when using this command, you will be prompted for a password for the far end machine after entering the command.

Usage Examples

The following example creates a port forward (between the AOS device and machine 10.10.10.1) using port **22** as the local forwarded port **7000** as the forward port on **10.10.10.1**. The user name on the remote machine is **MGARCIA**, and the password is **PASSWORD**

>**enable**
#ssh port-forward 7000 MGARCIA@10.10.10.1 password PASSWORD

ssh vrf

Use the **ssh vrf** command to create a secure shell (SSH) tunnel between the AOS unit and another device. Variations of this command include:

ssh vrf <*vrfName*><*url*><*interface*>
ssh vrf <*vrfName*><*url*>**myprivkey**
ssh vrf <*vrfName*><*url*>**myprivkey**
ssh vrf <*vrfName*><*url*>**myprivkey**<*private key for SSH authentication*>
ssh vrf <*vrfName*><*url*>**myprivkey** dsa
ssh vrf <*vrfName*><*url*>**myprivkey** ecdsa256
ssh vrf <*vrfName*><*url*>**myprivkey** ecdsa384
ssh vrf <*vrfName*><*url*>**myprivkey** ecdsa521
ssh vrf <*vrfName*><*url*>**myprivkey** rsa
ssh vrf <*vrfName*><*url*>**myprivkey** rsa-sha2-512
ssh vrf <*vrfName*><*url*>**port** <*port number: 1-65535*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> <*SSH authentication*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> **myprivkey** <*key for SSH authentication*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> **myprivkey dsa**
ssh vrf <*vrfName*><*url*>**port** <*port number*> **myprivkey ecdsa256**
ssh vrf <*vrfName*><*url*>**port** <*port number*> **myprivkey ecdsa384**
ssh vrf <*vrfName*><*url*>**port** <*port number*> **myprivkey ecdsa521**
ssh vrf <*vrfName*><*url*>**port** <*port number*> **myprivkey rsa**
ssh vrf <*vrfName*><*url*>**port** <*port number*> **myprivkey rsa-sha2-512**
ssh vrf <*vrfName*><*url*>**port** <*port number*> **privkey** <*private key file name*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> **source-interface** <*interface*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> **source-interface bvi** <*Bridged virtual interface number*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> **source-interface gigabit-ethernet** <*Gigabit Ethernet interface slot/port*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> **source-interface ppp** <*PPP interface number*>
ssh vrf <*vrfName*><*url*>**port** <*port number*> **source-interface tunnel** <*Tunnel interface number: 1-1024*>

Syntax Description

vrf	Specifies the name of the virtual routing and forwarding (VRF) network device.
<url>	Specifies the uniform resource locator (URL) of the far end listening address. The format of the URL string must be **user@server:remote-port**, for example, MGARCIA@10.10.10.1:7000. Optionally, you may include the IP address of an interface on the remote machine using the format **user@server:remote-port:FarEndListenAddress**, for example, MGARCIA@10.10.10.1:7000:10.10.10.2. If a far end listen address is not included as part of the URL, localhost is assumed and only those users logged into the remote machine can use the tunnel.

myprivkey	Optional. Specifies to use the AOS unit's DSA, RSA, rsa-sha512, ecdsa256, ecdsa384, and ecdsa521 private key for key SSH authentication.
port <*port*>	Optional. Specifies a port to use for the underlying SSH protocol instead of the default SSH port 22. Valid range is **1** to **65535**.
privkey <*filename*>	Optional. Specifies a private key file to use for SSH authentication.
Source-interface	Specifies the source interface. Specify an interface for the SSH connection.

Default Values

No default values are necessary for this command.

Command History

Release R12.2.0	Command was introduced.
Release 14.4.0	Command was expanded to include **myprivkey**, **dsa**, **rsa**, **ecdsa256**, **ecdsa384**, and **ecdsa521** key type options.

Functional Notes

If you do not specify a password when using this command, you will be prompted for a password from the far end machine after entering the command.

Usage Examples

The following example creates the SSH VRF (between the AOS device and machine 10.10.10.1) using port **22** as the local forwarded port. The VRF file name is TEST and user name is **MARCIA** on the remote machine **Adtran@10.10.10.1** with a **myprivkey** value is ecdsa256.

>**enable**
#ssh vrf TEST MARCIA@Adtran10.10.10.1
#ssh vrf TEST MARCIA@Adtran10.10.10.1 myprivkey
#ssh vrf TEST MARCIA@Adtran10.10.10.1myprivkey ecdsa256

The following example creates a SSH VRF (between the AOS device and machine 10.10.10.1) using port **22** as the local forwarded port and a **myprivkey** value is **dsa**.

#ssh vrf TEST MARCIA@Adtran10.10.10.1 port 22 myprivkey dsa

The following example creates a SSH VRF (between the AOS device and machine 10.10.10.1) using port **22** as the local forwarded port and a **source-interface** of **bvi**.

#ssh vrf TEST MARCIA@Adtran10.10.10.1 port 22 source-interface bvi

telnet

Use the **telnet** command to open a Telnet session (through AOS) to another system on the network. Variations of this command include the following:

telnet <*ip address* | *hostname*>
telnet <*ip address* | *hostname*> **port** <*tcp port*>
telnet vrf <*name*> <*ip address* | *hostname*>
telnet vrf <*name*> <*ip address* | *hostname*> **port** <*tcp port*>

Syntax Description

<*ip address* | *hostname*>	Specifies the IP address or host name of the remote system. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
port <*tcp port*>	Optional. Specifies the Transmission Control Protocol (TCP) port number to be used when connecting to a host through Telnet. Range is **1** to **65535**.
vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) where the IP address or host name exists.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 14.1	Command was expanded to specify the port number.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example opens a Telnet session with a remote system (**10.200.4.15**):

>**enable**
#telnet 10.200.4.15
User Access Login:
Password:

The following example opens a Telnet session with a remote system (**10.200.4.15**) on port **8010**:

>**enable**
#telnet 10.200.4.15 port 8010
User Access Login:
Password:

telnet stack-member <*unit id*>

Use the **telnet stack-member** command to Telnet to a stack member.

Syntax Description

<*unit id*>	Specifies unit ID of the stack member to connect via a Telnet session.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command is only available when in stack-master mode.

Usage Examples

The following example Telnets to a member of the stack:

>enable
#telnet stack-member 3
Trying Stack Member 3...Press Ctrl+C to abort

telnet vrf <*name*> stack-member <*number*>

Use the **telnet vrf stack-member** command to open a Telnet session (through AOS) with a member of the stack.

Syntax Description

vrf <*name*>	Specifies the virtual routing and forwarding (VRF) where the stack member exists.
stack-member <*number*>	Specifies which member of the stack to which to Telnet.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example opens a Telnet session with stack member **3** of the VRF **red**:

>**enable**
#telnet vrf red stack-member 3
Trying Stack Member 3...Press Ctrl+C to abort

terminal length *<number>*

The **terminal length** command sets the number of rows (lines) for a terminal session. Use the **no** form of this command to return to the default value. This command is only valid for the current session and returns to the default (24 rows) when the session closes.

Syntax Description

<number>	Specifies the number of rows for a terminal session. Range is **0** to **480** lines. Setting the **terminal length** to 0 disables paging.

Default Values

The default setting for this command is **24** rows.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sets the number of rows for a terminal session to **30**.

```
>enable
#terminal length 30
```

test cable-diagnostics

Use the **test cable-diagnostics** command to generate a report concerning various cabling states and issues related to the physical condition of an Ethernet cable connected to the specified port. Variations of this command include:

test cable-diagnostics switchport <*slot/port*>
test cable-diagnostics gigabit-switchport <*slot/port*>

Running a cable diagnostics test will disrupt traffic on the port being tested.

Syntax Description

switchport <*slot/port*>	Specifies that the cable diagnostics test be run on the indicated 10/100 Mbps switchport.
gigabit-switchport <*slot/port*>	Specifies that the cable diagnostics test be run on the indicated 10/100/1000 Mbps gigabit switchport.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example runs a cable diagnostics test on switchport **0/1**:

#test cable-diagnostics switchport 0/1

traceroute

Use the **traceroute** command to display the Internet Protocol version 4 (IPv4) routes a packet takes to reach the specified destination. Variations of this command include:

traceroute
traceroute [ip] <*ipv4 address* | *hostname*>
traceroute [ip] <*ipv4 address* | *hostname*> <*interface*>
traceroute [ip] <*ipv4 address* | *hostname*> **mef-ethernet** <*slot/port*>
traceroute [ip] <*ipv4 address* | *hostname*> **system-control-evc**
traceroute [ip] <*ipv4 address* | *hostname*> **system-management-evc**
traceroute [ip] <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
traceroute [ip] <*ipv4 address* | *hostname*> <*interface*> **source** <*ipv4 address*>
traceroute [ip] <*ipv4 address* | *hostname*> **mef-ethernet** <*slot/port*> <*ipv4 address*>
traceroute [ip] <*ipv4 address* | *hostname*> **system-control-evc source** <*ipv4 address*>
traceroute [ip] <*ipv4 address* | *hostname*> **system-management-evc source** <*ipv4 address*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> <*interface*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **mef-ethernet** <*slot/port*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **system-control-evc**
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **system-management-evc**
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **source** <*ipv4 address*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> <*interface*> **source** <*ipv4 address*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **mef-ethernet** <*slot/port*> <*ipv4 address*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **system-control-evc source** <*ipv4 address*>
traceroute [ip] vrf <*name*> <*ipv4 address* | *hostname*> **system-management-evc source** <*ipv4 address*>

Syntax Description

ip	Optional. Specifies an IPv4 trace.
<*interface*>	Optional. Specifies the egress interface to use for the trace. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **traceroute** <*ipv4 address* | *hostname*> **?** to display a list of valid interfaces.
mef-ethernet <*slot/port*>	Optional. Specifies the Metro Ethernet Forum (MEF) Ethernet interface is used for the trace.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC) is used for the trace.
system-management-evc	Optional. Specifies the system management EVC is used for the trace.
<*ipv4 address* | *hostname*>	Optional. Specifies the IPv4 address or host name of the remote system's route to trace.
source <*ipv4 address*>	Optional. Specifies the IPv4 address of the interface to use as the source of the trace. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) where the route exists.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command was expanded to include the <*interface*> and **ip** parameters.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

The **traceroute** command can be issued from both the Basic and Enable modes.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **traceroute** command:

```
>enable
#traceroute 192.168.0.1
Type CTRL+C to abort.
Tracing route to 192.168.0.1 over a maximum of 30 hops
  1   22ms   20ms   20ms    192.168.0.65
  2   23ms   20ms   20ms    192.168.0.1
```


traceroute ethernet

Use the **traceroute ethernet** command to initiate a linktrace message from one Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoint (MEP) to another MEP. These linktrace messages are used to trace the packet route to a destination MEP. Variations of this command include:

traceroute ethernet <*target-mac-address* | *target-mep-id*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **domain** <*domain name*> **association** <*association name*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **domain none association** <*association name*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **fdb-only**
traceroute ethernet <*target-mac-address* | *target-mep-id*> **interface** <*interface*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **mep** <*mep id*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **sorted**
traceroute ethernet <*target-mac-address* | *target-mep-id*> **timeout** <*timeout*>
traceroute ethernet <*target-mac-address* | *target-mep-id*> **ttl** <*value*>

After specifying the target for the linktrace messages, the other parameters can be entered in any order.

Syntax Description

<*target-mac-address* | *target-mep-id*>	Specifies the destination for the linktrace message. Medium access control (MAC) addresses are entered in the format **HH:HH:HH:HH:HH:HH**. Target MEP IDs are the unique numerical values identifying MEPs. MEP IDs range from **1** to **8191**.
domain <*domain name*>	Optional. Specifies the maintenance domain to which the transmitting MEP belongs.
domain none	Optional. Specifies no maintenance domain.
association <*association name*>	Optional. Specifies the maintenance association to which the transmitting MEP belongs.
fdb-only	Optional. Specifies that the maintenance points on the route only use their forwarding database, and not their continuity check message (CCM) database when deciding if/how to forward linktrace messages.
interface <*interface*>	Optional. Specifies the interface on which the transmitting MEP is configured. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**. For a list of appropriate interfaces, enter **interface ?** at the prompt.

mep <*mep id*>	Optional. Specifies the MEP ID of the transmitting MEP. MEP ID range is **1** to **8191**.
sorted	Optional. Specifies the traceroute utility waits until all traceroute results have been received and sorted by hop count before displaying them.
timeout <*timeout*>	Optional. Specifies the time that the MEP will wait for a response to the linktrace message. Range is **0** to **60** seconds.
ttl <*value*>	Optional. Specifies the time to live (TTL) field of the linktrace message. Range is **0** to **255**.

Default Values

By default, the **timeout** value is set to **5** seconds.

By default, the **ttl** value is set to **5** seconds.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface and the gigabit switchport interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

The **traceroute ethernet** command can be issued from both the Basic and Enable modes.

If the MEP ID is used as the target, the remote MEP must exist in the MEP CCM database (meaning the remote MEP is transmitting valid CCMs) so that the MEP ID can be translated to the MAC address before the linktrace message is transmitted.

Both the **domain** <*domain name*> and **association** <*association name*> parameters are not required if the source MEP ID of the MEP is specified and unique through the AOS device.

If the domain and association of the transmitting MEP are specified, and there is only one MEP in that domain or association, or if there is only one MEP configured on the unit, the **mep** <*mep id*> parameter is not required.

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example initiates the Ethernet traceroute utility from a MEP with the ID **1** to an MEP with an MEP ID of **201**:

>**enable**
#traceroute ethernet 201 mep 1

```
Type CTRL+C to abort.

TTL 255. LTM Timeout is 5 seconds
Tracing route to        MEPID 201 (00:10:94:00:00:06)
                from    MEPID 1
                in      Domain_1/MA_1
MD Level 7, vlan 0
Traceroute sent via interface eth 0/1

-------------------------------------------------------------------------------------------------------------------------------
Hops    Mac                             Flags           Ingress-Action          Relay Action
          PrevHop                                               Egress-Action
-------------------------------------------------------------------------------------------------------------------------------
1       00:10:94:00:00:00               Forwarded       InNoTLV                 RLY_MPDB
            00:A0:C8:16:96:0D                                   EgOK
3       00:10:94:00:00:05               Forwarded       InNoTLV                 RLY_MPDB
            00:10:94:00:00:04                                   EgOK
2       00:10:94:00:00:04               Forwarded       InNoTLV                 RLY_MPDB
            00:10:94:00:00:00                                   EgOK
4       00:10:94:00:00:06 (Eg)          Terminal        InNoTLV                 RLY_HIT
            00:10:94:00:00:05

Destination reached
```

Remember that linktrace can be a tree-structure, and is not always linear. The PrevHop for Hop 3 in the previous example tells you the MAC of Hop 2. This gives you a way to trace the linktrace message when a tree-structure exists. Refer to Section J.5 of IEEE 802.1ag for more information.

traceroute ipv6

Use the **traceroute ipv6** command to display the IPv6 nodes traversed to reach the specified destination. Variations of this command include:

traceroute ipv6 <*ipv6 address*>
traceroute ipv6 <*ipv6 address*> <*interface*>
traceroute ipv6 <*ipv6 address*> **mef-ethernet** <*slot/port*>
traceroute ipv6 <*ipv6 address*> **system-control-evc**
traceroute ipv6 <*ipv6 address*> **system-management-evc**
traceroute ipv6 <*ipv6 address*> <*interface*> **source** <*ipv6 address*>
traceroute ipv6 <*ipv6 address*> **mef-ethernet** <*slot/port*> <*ipv6 address*>
traceroute ipv6 <*ipv6 address*> **system-control-evc source** <*ipv6 address*>
traceroute ipv6 <*ipv6 address*> **system-management-evc source** <*ipv6 address*>
traceroute ipv6 <*ipv6 address*> **source** <*ipv6 address*>
traceroute ipv6 vrf <*name*> <*ipv6 address*>
traceroute ipv6 vrf <*name*> <*ipv6 address*> <*interface*>
traceroute ipv6 vrf <*name*> <*ipv6 address*> **mef-ethernet** <*slot/port*>
traceroute ipv6 vrf <*name*> <*ipv6 address*> **system-control-evc**
traceroute ipv6 vrf <*name*> <*ipv6 address*> **system-management-evc**
traceroute ipv6 vrf <*name*> <*ipv6 address*> <*interface*> **source** <*ipv6 address*>
traceroute ipv6 vrf <*name*> <*ipv6 address*> **mef-ethernet** <*slot/port*> **source** <*ipv6 address*>
traceroute ipv6 vrf <*name*> <*ipv6 address*> **system-control-evc source** <*ipv6 address*>
traceroute ipv6 vrf <*name*> <*ipv6 address*> **system-management-evc source** <*ipv6 address*>
traceroute ipv6 vrf <*name*> <*ipv6 address*> **source** <*ipv6 address*>

Syntax Description

<*interface*>	Optional. Specifies the egress interface when tracing a route to an IPv6 link-local address (any address that has the prefix **FE80::/64**). Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **traceroute ipv6** <*ipv6 address*> **?** to display a list of valid interfaces. This variable is ignored when using a non-link-local address.
<*ipv6 address*>	Specifies the IPv6 address of the remote system's route to trace. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. Entering the **traceroute ipv6** command using a link-local destination address prompts the user for an egress interface.
mef-ethernet <*slot/port*>	Optional. Specifies the Metro Ethernet Forum (MEF) Ethernet interface is used for the trace.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC) is used for the trace.
system-management-evc	Optional. Specifies the system management EVC is used for the trace.
source <*ipv6 address*>	Optional. Specifies the IPv6 address to use as the source address in the probing packets. The source IPv6 address must be a valid address local to the router on the specified virtual routing and forwarding (VRF) instance.

vrf <*name*>	Optional. Specifies the VRF where the IPv6 address exists.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

The **traceroute ipv6** command can be issued from both the Basic and Enable modes.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS platforms supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following is sample output from the **traceroute ipv6** command:

```
>enable
#traceroute ipv6 2001:DB8:1A0::3
Tracing route to over a maximum of 30 hops
Type CTRL+C to abort.
Legend:  '!' = Success, '?' = Unknown host, '$' = Invalid host address
         '*' = Request timed out, '-' = Destination host unreachable
         'x' = TTL expired in transit, 'e' = Unknown error
         'B' = Packet too big
1     2ms      2ms      3ms      2001:DB8:0:F820::5
2     102ms    109ms    102ms    2001:DB8:1A0::3
```

undebug all

Use the **undebug all** command to disable all activated debug messages.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example disables all activated debug messages:

```
>enable
#undebug all
```

verify-file

Use the **verify-file** command to validate a boot image file located in a specified memory location (CompactFlash®, system flash, RAM disk, or USB flash drive). AOS initiates the validation process automatically before an image can be set as the primary boot image. This command is used as a precautionary step before erasing the primary boot image. Variations of this command include:

verify-file cflash <*filename*>
verify-file flash <*filename*>
verify-file ramdisk <*filename*>
verify-file usbdrive0 <*filename*>

*Not all units are capable of using a RAM disk file system, CompactFlash card, or Universal Serial Bus (USB) flash drive. Use the **verify-file ?** command to display a list of valid commands at the enable prompt.*

Syntax Description

<*filename*>	Specifies the name of the file to validate.
cflash	Indicates the specified file is located on the CompactFlash card.
flash	Indicates the specified file is located in the system flash memory.
ramdisk	Indicates the specified file is located in the volatile RAM disk.
usbdrive0	Indicates the specified file is located in the USB flash drive memory.

Default Values

No default values are necessary for this command.

Command History

Release 17.7	Command was introduced.
Release 18.2	Command was expanded to include the **usbdrive0** parameter.
Release R12.1.0	Command version **verify-file flash** <*filename*> was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

The **verify-file flash** <*filename*> command is not available on vAOS instances.

Usage Examples

The following example validates the **NV3120A-17-05-01-00-E.biz** file (located in the volatile RAM disk) as a possible candidate for the boot system file:

>**enable**
#verify-file ramdisk NV3120A-17-05-01-00-E.biz
Valid file signature

vlan database

Use the **vlan database** command to enter the Virtual Local Area Network (VLAN) Database Configuration mode. Refer to the section *VLAN Database Command Set on page 3361* for more information.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enters the VLAN Configuration mode:

```
>enable
#vlan database
```


voice dsp capture

Use the **voice dsp capture** command to initiate digital signal processor (DSP) captures. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice dsp capture cancel
voice dsp capture start
voice dsp capture start <*value*>
voice dsp capture stop

Syntax Description

cancel	Cancels the current DSP capture and discards the captured files.
start	Starts the command line interface (CLI) wizard that prompts the user for the necessary information to initiate a DSP capture.
<*value*>	Optional. Specifies a DSP capture starting on a specific channel on DSP 0/1. The valid channel number range is **1** to **32**.
stop	Stops the current DSP capture and downloads the captured files to FLASH.

Default Values

By default, the DSP capture is disabled.

Command History

Release 15.1	Command was introduced.

Functional Notes

The voice DSP captures are used to help diagnose voice issues. The channel numbers for this command correspond to those seen in the **show** and **debug** commands (for example, the first channel is 1, not 0).

Output is received on all console sessions notifying you of a running DSP capture or download. Closing the CLI session on which the capture was started will cancel the current capture. This method of DSP capture is valid on AOS Release 15.1 or later, replacing the *en8 int voip 0/1* method.

Usage Examples

The following example starts a DSP capture:

#voice dsp capture start
DSP Slot [0]: **0**
DSP Port [1]: **1**
DSP Channel [1]:**1**
%Warning! Performance of this unit may be degraded during a DSP capture!
Continue and start DSP Capture? [y/n] **y**
DSP UTILITIES. Voice Capture A DSP capture is active on VoIP 0/1 on channel 1dsp capture

voice loopback-call

Use the **voice loopback-call** command to initiate and terminate voice loopback calls. Variations of this command include:

voice loopback-call start from <*number*> **to** <*number*>
voice loopback-call stop account <*number*>
voice loopback-call stop all
voice loopback-call stop id <*number*>

Syntax Description

start from <*number*>	Starts a loopback call from the specified extension number (loopback account).
to <*number*>	Specifies the extension number to call.
stop	Stops active loopback calls.
account <*number*>	Terminates the call(s) for the specific account.
all	Terminates all loopback calls.
id <*number*>	Terminates a specific loopback call based on the identity number of the call.

Default Values

By default, no loopback accounts are configured.

Command History

Release A1	Command was introduced.

Usage Examples

The following example starts a voice loopback call:

>**enable**
#voice loopback-call start from 5555 to 6100

wall *<message>*

Use the **wall** command to send messages to all users currently logged into the AOS unit.

Syntax Description

<message>	Sends a message to all users logged into the command line interface (CLI).

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sends the message “Reboot in 5 minutes if no objections” to the CLI screen of everyone currently connected:

>enable
#wall Reboot in 5 minutes if no objections

write

Use the **write** command to save the running configuration to the unit's nonvolatile random access memory (NVRAM) or a Trivial File Transfer Protocol (TFTP) server. Also, use the **write** command to clear NVRAM or to display the running configuration on the terminal screen. Entering the **write** command with no other arguments copies your configuration changes to the unit's NVRAM. Once the save is complete, the changes are retained even if the unit is shut down or suffers a power outage. Variations of this command include:

write
write dynvoice-config
write erase
write memory
write network
write terminal

Syntax Description

dynvoice-config	Optional. Writes dynvoice configuration information to the unit's NVRAM.
erase	Optional. Erases the configuration files saved to the unit's NVRAM.
memory	Optional. Saves the current configuration to NVRAM.
network	Optional. Saves the current configuration to the network TFTP server.
terminal	Optional. Displays the current configuration on the terminal screen.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example saves the current configuration to the unit's NVRAM:

```
>enable
#write memory
```

GLOBAL CONFIGURATION MODE COMMAND SET

To activate the Global Configuration mode, enter the **configure terminal** command at the Enable mode prompt. For example:

```
>enable
#configure terminal
(config)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

All other commands for this command set are described in this section in alphabetical order.

aaa accounting commands *<level>*

Use the **aaa accounting commands** command to create and define a default or named accounting method list for use with authentication, authorization, and accounting (AAA) accounting services. The accounting commands method lists specify the types of information recorded when users access specified command levels (privileged or unprivileged). Use the **no** form of this command to disable the accounting commands method list. Variations of this command include:

aaa accounting commands *<level>* **default none**
aaa accounting commands *<level>* **default stop-only group** *<name>*
aaa accounting commands *<level>* **default stop-only group tacacs+**
aaa accounting commands *<level>* *<listname>* **none**
aaa accounting commands *<level>* *<listname>* **stop-only group** *<name>*
aaa accounting commands *<level>* *<listname>* **stop-only group tacacs+**

Syntax Description

<level>	Specifies whether the method list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
<listname>	Creates and names the accounting commands method list to use rather than the default list.
default	Creates and defines the default accounting commands method list to use rather than a named list.
none	Specifies that no accounting methods are used.
stop-only	Records accounting information only when the connection terminates.
group *<name>*	Specifies using a subset of terminal access controller access-control system (TACACS+) servers for keeping accounting records. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.
group tacacs+	Specifies using all TACACS+ servers for keeping accounting records. TACACS+ servers must be configured to use this method. Refer to the *Functional Notes* for more information.

Default Values

By default, AAA accounting is disabled and no accounting command method lists are defined.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA accounting is an AAA service that helps track the services and resources that network users are accessing and using. Accounting works by sending records of user activity to a configured server that can be used by network administrators to monitor network management, client billing, and auditing. In AOS, AAA accounting can record the commands users are entering using the **aaa accounting commands** command to create method lists that monitor specified command levels.

Before AAA accounting method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA accounting method list relies on a combination of accounting methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** *<name>* method that can be entered multiple times to accommodate multiple configured server groups. When specifying methods for the AAA accounting commands method list, it is important to remember that no additional parameters are available when using the **none** option, and that **group tacacs+** or **group** *<name>* methods are not available until after specifying **stop-only**. Once you have specified **stop-only** as a method, you can specify **group tacacs+** and **group** *<name>* in any order or combination. If the unit fails to make a connection with the first group listed, it will try the next group specified.

The two types of method lists created using the **aaa accounting commands** command are a default list and a named list. A default list is one that is created and automatically applied to all line interfaces at the global level. A named method list is one that does not perform any action until it is manually applied to an interface. Named AAA accounting commands method lists are applied to line interfaces using the **accounting commands** command from the appropriate line interface configuration mode (*Line (Console) Interface Command Set on page 2021*, *Line (Telnet) Interface Command Set on page 2054*, or *Line (SSH) Interface Command Set on page 2038*).

To use TACACS+ servers to record command accounting information (TACACS+ are the only servers available for AOS AAA accounting; RADIUS servers are not supported), the TACACS+ servers must be configured prior to creating the method list. You can configure all TACACS+ servers in the system using the command *tacacs-server on page 1867*. You can configure individual TACACS+ servers using the command *tacacs-server host on page 1868*. Once the TACACS+ servers have been configured, you can use all TACACS+ servers for maintaining accounting records by using the **group tacacs+** method. If you only want to use some of the available TACACS+ servers for accounting, you can create a named server group and add the TACACS+ servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *TACACS+ Group Command Set on page 4507*.

For more information about AAA accounting, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a list called **myList** and specifies that accounting records are generated for all Level **1** commands when the connection terminates, and that these records are received by all configured TACACS+ servers:

(config)**#aaa accounting commands 1 myList stop-only group tacacs+**

aaa accounting connection

Use the **aaa accounting connection** command to create and define a default or named accounting method list for use with authentication, authorization, and accounting (AAA) accounting services. The accounting connection method lists are used to specify the types of information recorded about outbound connections made from the AOS unit. Use the **no** form of this command to disable the accounting connection method list. Variations of this command include:

aaa accounting connection default none
aaa accounting connection default start-stop group *<name>*
aaa accounting connection default start-stop group tacacs+
aaa accounting connection default stop-only group *<name>*
aaa accounting connection default stop-only group tacacs+
aaa accounting connection *<listname>* **none**
aaa accounting connection *<listname>* **start-stop group** *<name>*
aaa accounting connection *<listname>* **start-stop group tacacs+**
aaa accounting connection *<listname>* **stop-only group** *<name>*
aaa accounting connection *<listname>* **stop-only group tacacs+**

Syntax Description

default	Creates and defines the default accounting connection method list to use rather than the named list.
<listname>	Creates and names the accounting connection method list to create and use rather than the default list.
none	Specifies that no accounting methods are used.
start-stop	Records accounting information when the connection begins and when the connection terminates.
stop-only	Records accounting information only when the connection terminates.
group *<name>*	Specifies using a subset of terminal access controller access-control system (TACACS+) servers for keeping accounting records. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.
group tacacs+	Specifies using all TACACS+ servers for keeping accounting records. TACACS+ servers must be configured to use this method. Refer to the *Functional Notes* for more information.

Default Values

By default, AAA accounting connection is disabled and no accounting connection method lists are defined.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA accounting is an AAA service that helps track the services and resources that network users are accessing and using. Accounting works by sending records of user activity to a configured server that can be used by network administrators to monitor network management, client billing, and auditing. In AOS, AAA accounting can record information about outbound connections made from the network access server using the **aaa accounting connection** command to create method lists that monitor outbound connections.

Before AAA accounting method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA accounting method list relies on a combination of accounting methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** <*name*> method that can be entered multiple times to accommodate multiple configured server groups. When specifying methods for the AAA accounting connection method list, it is important to remember that no additional parameters are available when using the **none** option, and that **group tacacs+** or **group** <*name*> methods are not available until after specifying **start-stop** or **stop-only**. Once you have specified **start-stop** or **stop-only** as a method, you can specify **group tacacs+** and **group** <*name*> in any order or combination. If the unit fails to make a connection with the first group listed, it will try the next group specified.

The two types of method lists created using the **aaa accounting connection** command are a default list and a named list. A default list is one that is created and automatically applied to all line interfaces at the global level. A named method list is one that does not perform any action until it is manually applied to an interface. Named AAA accounting connection method lists are applied to line interfaces using the **accounting connection** command from the appropriate line interface configuration mode (*Line (Console) Interface Command Set on page 2021*, *Line (Telnet) Interface Command Set on page 2054*, or *Line (SSH) Interface Command Set on page 2038*).

To use TACACS+ servers to record connection accounting information (TACACS+ are the only servers available for AOS AAA accounting; RADIUS servers are not supported), the TACACS+ servers must be configured prior to creating the method list. You can configure all TACACS+ servers in the system using the command *tacacs-server on page 1867*. You can configure individual TACACS+ servers using the command *tacacs-server host on page 1868*. Once the TACACS+ servers have been configured, you can use all TACACS+ servers for maintaining accounting records by using the **group tacacs+** method. If you only want to use some of the available TACACS+ servers for accounting, you can create a named server group and add the TACACS+ servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *TACACS+ Group Command Set on page 4507*.

For more information about AAA accounting, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a list called **myList** and sends the connection information to all TACACS+ servers when the connection terminates:

(config)**#aaa accounting connection myList stop-only group tacacs+**

The following example creates a list called **myList** and sends the connection information to the TACACS+ servers when the connection is made and when the connection terminates:

(config)**#aaa accounting connection myList start-stop group tacacs+**

aaa accounting exec

Use the **aaa accounting exec** command to create and define a default or named accounting method list for use with authentication, authorization, and accounting (AAA) accounting services. AAA executive accounting method lists are used to specify the types of information recorded about inbound connections made by connecting to the line interfaces and creating a terminal session. Use the **no** form of this command to disable the accounting exec method list. Variations of this command include:

aaa accounting exec default none
aaa accounting exec default start-stop group *<name>*
aaa accounting exec default start-stop group tacacs+
aaa accounting exec default stop-only group *<name>*
aaa accounting exec default stop-only group tacacs+
aaa accounting exec *<listname>* **none**
aaa accounting exec *<listname>* **start-stop group** *<name>*
aaa accounting exec *<listname>* **start-stop group tacacs+**
aaa accounting exec *<listname>* **stop-only group** *<name>*
aaa accounting exec *<listname>* **stop-only group tacacs+**

Syntax Description

default	Creates and defines the default accounting exec method list to use rather than the named list.
<listname>	Creates and names the accounting exec method list to use rather than the default list.
none	Specifies that no accounting methods are used.
start-stop	Records accounting information when the connection begins and when the connection terminates.
stop-only	Records accounting information only when the connection terminates.
group *<name>*	Specifies using a subset of terminal access controller access-control system (TACACS+) servers for keeping accounting records. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.
group tacacs+	Specifies using all TACACS+ servers for keeping accounting records. TACACS+ servers must be configured to use this method. Refer to the *Functional Notes* for more information.

Default Values

By default, AAA accounting exec is disabled and no accounting exec method lists are defined.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA accounting is an AAA service that helps track the services and resources that network users are accessing and using. Accounting works by sending records of user activity to a configured server that can be used by network administrators to monitor network management, client billing, and auditing. In AOS, AAA accounting can record information about inbound connections (made by connecting to the line interfaces and creating a terminal session) using the **aaa accounting exec** command to create method lists that monitor inbound connections.

Before AAA accounting method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA accounting method list relies on a combination of accounting methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** <*name*> method that can be entered multiple times to accommodate multiple configured server groups. When specifying methods for the AAA accounting exec method list, it is important to remember that no additional parameters are available when using the **none** option, and that **group tacacs+** or **group** <*name*> methods are not available until after specifying **start-stop** or **stop-only**. Once you have specified **start-stop** or **stop-only** as a method, you can specify **group tacacs+** and **group** <*name*> in any order or combination. If the unit fails to make a connection with the first group listed, it will try the next group specified.

The two types of method lists created using the **aaa accounting exec** command are a default list and a named list. A default list is one that is created and automatically applied to all line interfaces at the global level. A named method list is one that does not perform any action until it is manually applied to an interface. Named AAA accounting exec method lists are applied to line interfaces using the **accounting exec** command from the appropriate line interface configuration mode(*Line (Console) Interface Command Set on page 2021*, *Line (Telnet) Interface Command Set on page 2054*, or *Line (SSH) Interface Command Set on page 2038*).

To use TACACS+ servers to record exec accounting information (TACACS+ are the only servers available for AOS AAA accounting; RADIUS servers are not supported), the TACACS+ servers must be configured prior to creating the method list. You can configure all TACACS+ servers in the system using the command *tacacs-server on page 1867*. You can configure individual TACACS+ servers using the command *tacacs-server host on page 1868*. Once the TACACS+ servers have been configured, you can use all TACACS+ servers for maintaining accounting records by using the **group tacacs+** method. If you only want to use some of the available TACACS+ servers for accounting, you can create a named server group and add the TACACS+ servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *TACACS+ Group Command Set on page 4507*.

For more information about AAA accounting, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a list called **myList** and sends the connection/login records to the TACACS+ servers when the connection is terminated:

(config)**#aaa accounting exec myList stop-only group tacacs+**

aaa accounting suppress null-username

Use the **aaa accounting suppress null-username** command to specify that authentication, authorization, and accounting (AAA) accounting records for users with a NULL user name are not sent to the AAA accounting server.

Syntax Description

No subcommands.

Default Values

By default, records of all user accounts, including NULL user names, are sent to the server.

Command History

Release 11.1	Command was introduced.

Functional Notes

Null users are those users whose user name string is NULL. Users might have this user name if they came in on a line whose record type is **none** (typically, these are users that authenticated with a password-only login or no login).

Usage Examples

The following example specifies that users with the user name NULL are not sent to the server:

(config)**#aaa accounting suppress null-username**

aaa accounting update

Use the **aaa accounting update** command to specify how often authentication, authorization, and accounting (AAA) accounting records are sent to the accounting server(s). Use the **no** form of this command to return to the default setting. Variations of this command include:

aaa accounting update newinfo
aaa accounting update periodic <*value*>

Syntax Description

newinfo	Specifies that information is sent to the server only when there is new recorded information.
periodic <*value*>	Specifies the time interval (in minutes) between sending accounting records to the server. Interval range is **1** to **2147483647**.

Default Values

By default, accounting records are sent to the server every **5** minutes.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies that accounting records are sent to the accounting server every **60** minutes:

(config)**#aaa accounting update periodic 60**

aaa authentication banner <*banner*>

Use the **aaa authentication banner** command to specify the banner shown during authentication, authorization, and accounting (AAA) login/authentication. Using the **no** form of this command returns the banner to the default message.

Syntax Description

banner <*banner*>	Sets the banner shown before user authentication is attempted. The banner can be multiple lines. Enter a delimiter (such as #) to begin recording the typed text message used for the banner. The message must end with the same delimiter to indicate that the message is complete. The text delimiters are not displayed to the screen during operation.

Default Values

By default, the authentication banner is **User Access Verification**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example changes the authentication banner to read **User Login Authentication**:

(config)#**aaa authentication banner #**
Enter TEXT message. End with the character '#'.
User Login Authentication:#
(config)#

aaa authentication enable default

Use the **aaa authentication enable default** command to create and define the default authentication, authorization, and accounting (AAA) authentication method list used for access to the Enable (privileged) mode. Use the **no** form of this command to disable the authentication method list. Variations of this command include:

aaa authentication enable default enable
aaa authentication enable default group radius
aaa authentication enable default group tacacs+
aaa authentication enable default group <*name*>
aaa authentication enable default line
aaa authentication enable default none

*Each method parameter after **default** specifies the authentication method to be attempted in the order in which they are to be tried. Multiple methods can be specified for authentication, but the authentication procedure is dependent upon the entry order of the methods.*

Syntax Description

none	Specifies that no authentication methods are used. If this method is entered, it should come at the end of the list of authentication methods in the command entry. This method should only be used to prevent a lock-out situation.
line	Specifies using the line password (Telnet 0 through 4 or console 0 through 1) for authentication. The line password must be configured to use this method (using the **password** <*password*> command from the appropriate line interface configuration mode prompt).
enable	Specifies using the Enable mode password for authentication. The Enable mode password must be defined to use this method (using the command *enable password <password> on page 1270*).
group radius	Specifies that all defined remote authentication dial-in user service (RADIUS) servers are used for authentication. RADIUS servers must be configured to use this method. Refer to the *Functional Notes* for more information.
group tacacs+	Specifies that all defined terminal access controller access-control system plus (TACACS+) servers are used for authentication. TACACS+ servers must be configured to use this method. Refer to the *Functional Notes* for more information.
group <*name*>	Specifies using a subset of TACACS+ or RADIUS servers for authentication. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.

Default Values

If the Enable mode password is used as an authentication method and the authentication request is going to a RADIUS server, the user name **$enabl15$**is sent by default. If the request is going to a TACACS+ server, the user name used for login authentication is sent by default.

If no default methods list is configured, the unit uses the Enable mode password for authentication. If no password is configured, consoles are allowed access (this prevents a lock-out condition).

Command History

Release 5.1	Command was introduced.
Release 11.1	The **group tacacs+** command was added.

Functional Notes

AAA authentication is an AAA service that helps verify user logins, user access to the Enable mode, and port usage. Authentication works by verifying user credentials with those stored on a server. In AOS, AAA authentication can verify a user's permission to access Enable mode by using the **aaa authentication enable default** command to create the default method list that monitors user permissions.

Before AAA authentication method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA authentication method list relies on a combination of authentication methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** <*name*> method that can be entered multiple times to accommodate multiple configured server groups. If the unit fails to make a connection with the first group listed, it will try the next group specified.

*For security reasons, Adtran recommends that the **local** authentication method be used instead of the **none** authentication method. Using the **local** authentication method prevents unauthorized users from gaining access to the device during a period in which the links to all authentication servers are down. The local user database contained within the AOS device will always be available and serves as the last line of defense.*

The type of method lists created using the **aaa authentication enable default** command is a default list. A default list is one that is created and automatically applied to all line interfaces at the global level.

To use TACACS+ servers to perform Enable mode authentication, the TACACS+ servers must be configured prior to creating the method list. You can configure all TACACS+ servers in the system using the command *tacacs-server on page 1867*. You can configure individual TACACS+ servers using the command *tacacs-server host on page 1868*. Once the TACACS+ servers have been configured, you can use all TACACS+ servers for authentication by using the **group tacacs+** method. If you only want to use some of the available TACACS+ servers for authentication, you can create a named server group and add the TACACS+ servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *TACACS+ Group Command Set on page 4507*.

To use RADIUS servers to perform Enable mode authentication, the RADIUS servers must be configured prior to creating the method list. You can configure all RADIUS servers in the system using the command *radius-server on page 1680*. You can configure individual RADIUS servers using the command *radius-server host on page 1682*. Once the RADIUS servers have been configured, you can use all RADIUS servers for authentication by using the **group radius** method. If you only want to use some of the available RADIUS servers for authentication, you can create a named server group and add the RADIUS servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *RADIUS Group Command Set on page 4498*.

For more information about AAA authentication, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies using the line password as the first method of authentication and using the Enable mode password as the second:

(config)**#aaa authentication enable default line enable**

aaa authentication fail-message *<message>*

Use the **aaa authentication fail-message** command to specify the authentication, authorization, and accounting (AAA) authentication fail message. This message is displayed if user authentication fails. Use the **no** form of this command to return to the default message.

Syntax Description

<message>	Specifies the message shown if user authentication fails. The message can be multiple lines. Enter a delimiter (such as **#**) to begin recording the typed text message displayed after a failed authentication attempt. The message must end with the same delimiter to indicate that the message is complete. The text delimiters are not displayed to the screen during operation.

Default Values

By default, the authentication fail message banner is set to **Authentication failed**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example changes the authentication fail message to **Failed Authentication. Please try again.**:

(config)**#aaa authentication fail-message #**
Enter TEXT message. End with the character '**#**'.
Failed Authentication. Please try again.
(config)#

aaa authentication login

Use the **aaa authentication login** command to create and define a default or named method list for use with authentication, authorization, and accounting (AAA) authentication services. The AAA authentication login method list specifies the methods used to authenticate a user upon login. Use the **no** form of this command to disable the authentication login method list. Variations of this command include:

aaa authentication login default enable
aaa authentication login default group radius
aaa authentication login default group tacacs+
aaa authentication login default group *<name>*
aaa authentication login default line
aaa authentication login default local
aaa authentication login default none
aaa authentication login *<listname>* **enable**
aaa authentication login *<listname>* **group radius**
aaa authentication login *<listname>* **group tacacs+**
aaa authentication login *<listname>* **group** *<name>*
aaa authentication login *<listname>* **line**
aaa authentication login *<listname>* **local**
aaa authentication login *<listname>* **none**

*Each method parameter after **default** or <listname> specifies the authentication method to be attempted in the order in which they are to be tried. Multiple methods can be specified for authentication, but the authentication procedure is dependent upon the entry order of the methods.*

Syntax Description

default	Creates and defines the default login authentication method list to use rather than a named list.
<listname>	Creates and names the login authentication method list to use rather than the default list.
none	Specifies that no authentication methods are used. If this method is entered, it should come at the end of the list of authentication methods in the command entry. This method should only be used to prevent a lock-out situation.
line	Specifies using the line password (Telnet 0 through 4 or console 0 through 1) for authentication. The line password must be configured to use this method (using the **password** *<password>* command from the appropriate line interface configuration mode prompt).
enable	Specifies using the Enable mode password for authentication. The Enable mode password must be defined to use this method (using the command *enable password <password> on page 1270*).

local	Specifies using the local user name for authentication. User names must be in the local user name database to use this method. User names are set using the command *username <username> password <password> on page 1887*.
group radius	Specifies that all defined remote authentication dial-in user service (RADIUS) servers are used for authentication. RADIUS servers must be configured to use this method. Refer to the *Functional Notes* for more information.
group tacacs+	Specifies that all defined terminal access controller access-control system plus (TACACS+) servers are used for authentication. TACACS+ servers must be configured to use this method. Refer to the *Functional Notes* for more information.
group <*name*>	Specifies using a subset of TACACS+ or RADIUS servers for authentication. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.

Default Values

By default, AAA authentication login method lists are not defined. Once a default list is defined, it is automatically applied to all line interfaces unless a named list is created and applied manually.

Command History

Release 5.1	Command was introduced.
Release 11.1	The **group tacacs+** command was added.

Functional Notes

AAA authentication is an AAA service that helps verify user logins, user access to the Enable mode, and port usage. Authentication works by verifying user credentials with those stored on a server. In AOS, AAA authentication can verify a user's permission to access the unit by using the **aaa authentication login** command to create a method list that monitors user access permissions.

Before AAA authentication method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA authentication method list relies on a combination of authentication methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** <*name*> method that can be entered multiple times to accommodate multiple configured server groups. If the unit fails to make a connection with the first group listed, it will try the next group specified.

*For security reasons, Adtran recommends that the **local** authentication method be used instead of the **none** authentication method. Using the **local** authentication method prevents unauthorized users from gaining access to the device during a period in which the links to all authentication servers are down. The local user database contained within the AOS device will always be available and serves as the last line of defense.*

The two types of method lists created using the **aaa authentication login** command are a default list and a named list. A default list is one that is created and automatically applied to all line interfaces at the global level. A named method list is one that does not perform any action until it is manually applied to an interface. Named AAA login authentication method lists are applied to line interfaces using the **login authentication** <*listname*> command from the appropriate line interface configuration mode (*Line (Console) Interface Command Set on page 2021*, *Line (Telnet) Interface Command Set on page 2054*, or *Line (SSH) Interface Command Set on page 2038*).

To use TACACS+ servers to perform login authentication, the TACACS+ servers must be configured prior to creating the method list. You can configure all TACACS+ servers in the system using the command *tacacs-server on page 1867*. You can configure individual TACACS+ servers using the command *tacacs-server host on page 1868*. Once the TACACS+ servers have been configured, you can use all TACACS+ servers for authentication by using the **group tacacs+** method. If you only want to use some of the available TACACS+ servers for authentication, you can create a named server group and add the TACACS+ servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *TACACS+ Group Command Set on page 4507*.

To use RADIUS servers to perform login authentication, the RADIUS servers must be configured prior to creating the method list. You can configure all RADIUS servers in the system using the command *radius-server on page 1680*. You can configure individual RADIUS servers using the command *radius-server host on page 1682*. Once the RADIUS servers have been configured, you can use all RADIUS servers for authentication by using the **group radius** method. If you only want to use some of the available RADIUS servers for authentication, you can create a named server group and add the RADIUS servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *RADIUS Group Command Set on page 4498*.

For more information about AAA authentication, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a login authentication list called **myList** and specifies using the **local** database as the first method, **myGroup** as the second method, and **line** password as the third method for login authentication:

(config)**#aaa authentication login myList local group myGroup line**

The following command sets the **default** authentication list for logins to use the **local** database as the first authentication method:

(config)**#aaa authentication login default local**

aaa authentication password-prompt <*prompt*>

Use the **aaa authentication password-prompt** command to specify the message shown when prompting a user for their password during authentication, authorization, and accounting (AAA) authentication. The **no** form of this command returns the prompt to the default prompt.

Syntax Description

<*prompt*>	Specifies the prompt that displays when prompting users for their password. Enter a single line of text enclosed in quotation marks.

Default Values

By default, the authentication password prompt is set to **Password:**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example specifies the authentication password prompt reads **Please Enter Your Password:**

(config)**#aaa authentication password-prompt "Please Enter Your Password:"**

aaa authentication port-auth default

Use the **aaa authentication port-auth default** command to create and define the default method list for use with authentication, authorization, and accounting (AAA) port authentication services. Use the **no** form of this command to disable the authentication list. Variations of this command include:

aaa authentication port-auth default group radius
aaa authentication port-auth default group <*name*>
aaa authentication port-auth default local
aaa authentication port-auth default none

*Each method parameter after **default** specifies the authentication method to be attempted in the order in which they are to be tried. Multiple methods can be specified for authentication, but the authentication procedure is dependent upon the entry order of the methods.*

Syntax Description

none	Specifies that no authentication methods are used. If this method is entered, it should come at the end of the list of authentication methods in the command entry. This method should only be used to prevent a lock-out situation.
local	Specifies using the local user name for port authentication. User names must be in the local user name database to use this method. User names are set using the command *username <username> password <password> on page 1887*.
group radius	Specifies that all defined remote authentication dial-in user service (RADIUS) servers are used for authentication. RADIUS servers must be configured to use this method. Refer to the *Functional Notes* for more information.
group <*name*>	Specifies using a subset of RADIUS servers for port authentication. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.

Default Values

By default, no port authentication method lists are defined.

Command History

Release 10.1	Command was introduced.

Functional Notes

AAA authentication is an AAA service that helps verify user logins, user access to the Enable mode, and port usage. Authentication works by verifying user credentials with those stored on a server. In AOS, AAA authentication can verify port usage by using the **aaa authentication port-auth default** command to create the default method list that monitors port usage.

Before AAA authentication method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA authentication method list relies on a combination of authentication methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** <*name*> method that can be entered multiple times to accommodate multiple configured server groups. If the unit fails to make a connection with the first group listed, it will try the next group specified.

*For security reasons, Adtran recommends that the **local** authentication method be used instead of the **none** authentication method. Using the **local** authentication method prevents unauthorized users from gaining access to the device during a period in which the links to all authentication servers are down. The local user database contained within the AOS device will always be available and serves as the last line of defense.*

The type of method lists created using the **aaa authentication port-auth default** command is a default list. A default list is one that is created and automatically applied to all line interfaces at the global level.

To use RADIUS servers to perform port authentication, the RADIUS servers must be configured prior to creating the method list. You can configure all RADIUS servers in the system using the command *radius-server on page 1680*. You can configure individual RADIUS servers using the command *radius-server host on page 1682*. Once the RADIUS servers have been configured, you can use all RADIUS servers for authentication by using the **group radius** method. If you only want to use some of the available RADIUS servers for authentication, you can create a named server group and add the RADIUS servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *RADIUS Group Command Set on page 4498*.

For more information about AAA authentication, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the **local** user database be used for port authentication:

(config)**#aaa authentication port-auth default local**

aaa authentication username-prompt <*prompt*>

Use the **aaa authentication username-prompt** command to specify the message shown when prompting a user for their user name during authentication, authorization, and accounting (AAA) authentication. Use the **no** form of this command to return to the default prompt.

Syntax Description

<*prompt*>	Specifies the prompt that displays when prompting users for their user name. Enter a single line of text enclosed in quotation marks.

Default Values

By default, the authentication user name prompt is set to **Username:**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example specifies the authentication user name prompt reads **Please Enter Your User Name:**

(config)**#aaa authentication username-prompt “Please Enter Your User Name:”**

aaa authorization commands <*level*>

Use the **aaa authorization commands** command to create and define a default or named authorization method list for use with authentication, authorization, and accounting (AAA) authorization services. AAA command authorization method lists are used to allow or restrict the use of certain commands on a per-user basis. Use the **no** form of this command to disable the authorization commands method list. Variations of this command include:

aaa authorization commands <*level*> **default group tacacs+**
aaa authorization commands <*level*> **default group** <*name*>
aaa authorization commands <*level*> **default if-authenticated**
aaa authorization commands <*level*> **default none**
aaa authorization commands <*level*> <*listname*> **group tacacs+**
aaa authorization commands <*level*> <*listname*> **group** <*name*>
aaa authorization commands <*level*> <*listname*> **if-authenticated**
aaa authorization commands <*level*> <*listname*> **none**

*Each method parameter after **default** or <listname> specifies the authorization method to be attempted in the order in which they are to be tried. Multiple methods can be specified for authorization, but the authorization procedure is dependent upon the entry order of the methods.*

Syntax Description

<*level*>	Specifies whether the method list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
<*listname*>	Creates and names the authorization commands method list to use rather than the default list.
default	Creates and defines the default authorization commands method list to use rather than a named list.
none	Specifies that no authorization methods are used for command authorization. If this method is entered, it should come at the end of the list of authorization methods in the command entry. This method should only be used to prevent a lock-out situation.
if-authenticated	Specifies that authorization is successful if the user has already been authenticated. AAA authentication must be configured to use this method. Refer to the *Functional Notes* for more information.
group tacacs+	Specifies using all terminal access controller access-control system plus (TACACS+) servers for authorizing command usage. TACACS+ servers must be configured to use this method. Refer to the *Functional Notes* for more information.
group <*name*>	Specifies using a subset of TACACS+ servers for authorizing command usage. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.

Default Values

By default, no AAA authorization method lists are defined or applied.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA authorization is an AAA service that helps limit the network services available to users. Authorization works by retrieving information from the user's profile (stored either on the local database or security server) and uses that information to determine the areas of the network to which the user is allowed access. In AOS, AAA authorization can limit the commands available to a specific user and specify whether or not users can access privileged command line interface (CLI) sessions. Limiting available commands on a per-user basis is achieved by using the **aaa authorization commands** command to create a default or named method list that specifies which level of commands (Level **1** or Level **15**) are authorized.

The user command privilege level (1 or 15) must be defined in addition to specifying all of the commands available on a per-user basis in the configuration of the TACACS+ server. Commands of a particular level are not checked for authorization unless explicitly defined in the configuration with a method list. For example, if a method list is defined for Level 1 commands but not Level 15, then a user is able to enter any Level 15 commands since no authorization takes place due to the lack of a Level 15 commands method list. The same user will only be allowed to enter the Level 1 commands configured for the user in the Level 1 commands method list.

Before AAA authorization method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA authorization method list relies on a combination of authorization methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** <*name*> method that can be entered multiple times to accommodate multiple configured server groups. If the unit fails to make a connection with the first group listed, it will try the next group specified.

*For security reasons, Adtran recommends that the **local** authentication method be used instead of the **none** authentication method. Using the **local** authentication method prevents unauthorized users from gaining access to the device during a period in which the links to all authentication servers are down. The local user database contained within the AOS device will always be available and serves as the last line of defense.*

The two types of method lists created using the **aaa authorization commands** command are a default list and a named list. A default list is one that is created and automatically applied to all line interfaces at the global level. A named method list is one that does not perform any action until it is manually applied to an interface. Named AAA command authorization method lists are applied to line interfaces using the **authorization commands** *<level> <listname>* command from the appropriate line interface configuration mode (*Line (Console) Interface Command Set on page 2021*, *Line (Telnet) Interface Command Set on page 2054*, or *Line (SSH) Interface Command Set on page 2038*).

To use TACACS+ servers to perform command authorization, the TACACS+ servers must be configured prior to creating the method list. You can configure all TACACS+ servers in the system using the command *tacacs-server on page 1867*. You can configure individual TACACS+ servers using the command *tacacs-server host on page 1868*. Once the TACACS+ servers have been configured, you can use all TACACS+ servers for authorization by using the **group tacacs+** method. If you only want to use some of the available TACACS+ servers for authorization, you can create a named server group and add the TACACS+ servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *TACACS+ Group Command Set on page 4507*.

For more information about AAA authorization, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a command authorization method list called **myList**, which authorizes unprivileged commands (this succeeds only if the user has been authenticated successfully):

(config)**#aaa authorization commands 1 myList if-authenticated**

The following command defines the **default** command authorization method list to authorize privileged (level 15) commands against all defined TACACS+ servers:

(config)**#aaa authorization commands 15 default group tacacs+**

If command authorization is used in conjunction with a TACACS+ server, the same user name that is used to access AOS must be configured on the server.

aaa authorization config-command

Use the **aaa authorization config-command** command to enable or disable authorization for configuration mode commands in AOS authentication, authorization, and accounting (AAA) services. This command is used to verify that command-level authorization is enabled before applying AAA command authorization method lists to a specific line interface. Use the **no** form of this command to disable authorization for configuration commands.

Syntax Description

No subcommands.

Default Values

By default, authorization for configuration commands is enabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

The **aaa authorization config-command** command is used to ensure that authorization for configuration commands is enabled at the global level before applying any AAA authorization method lists to a line interface (console, Telnet, or secure shell (SSH)). This feature must be enabled before AAA authorization method lists can be applied to the interface.

For more information about AAA authorization, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables authorization of configuration mode commands:

(config)**#aaa authorization config-command**

aaa authorization console

Use the **aaa authorization console** command to enable AOS authentication, authorization, and accounting (AAA) on the console interface. This command is used to verify that the console interface will allow AAA operation before an AAA authorization method list is applied to the console interface. Use the **no** form of this command to disable AAA on the console interface.

Syntax Description

No subcommands.

Default Values

By default, authorization is disabled on a console line interface. This measure prevents accidental lockout issues on directly connected lines.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA authorization method lists cannot be applied to a console interface until the **aaa authorization console** command has been issued.

For more information about AAA authorization, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables AAA authorization use on console interfaces:

(config)**#aaa authorization console**

aaa authorization exec

Use the **aaa authorization exec** command to create and define a default or named authorization method list for use with authentication, authorization, and accounting (AAA) authorization services. The authorization exec method list sets the parameters for authorizing access to the Enable mode in the command line interface (CLI). Use the **no** form of this command to disable the authorization method list. Variations of this command include:

aaa authorization exec default group <*name*>
aaa authorization exec default group tacacs+
aaa authorization exec default if-authenticated
aaa authorization exec default none
aaa authorization exec <*listname*> **group** <*name*>
aaa authorization exec <*listname*> **group tacacs+**
aaa authorization exec <*listname*> **if-authenticated**
aaa authorization exec <*listname*> **none**

*Each method parameter after **default** or <listname> specifies the authorization method to be attempted in the order in which they are to be tried. Multiple methods can be specified for authorization, but the authorization procedure is dependent upon the entry order of the methods.*

Syntax Description

default	Creates and defines the default authorization method list to use rather than a named method list.
<*listname*>	Creates and names the authorization method list to use rather than the default list.
none	Specifies that no authorization methods are used for executive authorization. If this method is entered, it should come at the end of the list of authorization methods in the command entry. This method should only be used to prevent a lock-out situation.
if-authenticated	Specifies that authorization is successful if the user has already been authenticated. AAA authentication must be configured to use this method.
group tacacs+	Specifies using all terminal access controller access-control system plus (TACACS+) servers for authorizing executive CLI privileges. TACACS+ servers must be configured to use this method. Refer to the *Functional Notes* for more information.
group <*name*>	Specifies using a subset of TACACS+ servers for authorizing executive CLI privileges. Subsets are named server groups previously created using the command *aaa group server on page 1184*. A server group must be configured to use this method.

Default Values

By default, AAA authorization for executive CLI privileges is disabled and no authorization method lists are defined.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA authorization is an AAA service that helps limit the network services available to users. Authorization works by retrieving information from the user's profile (stored either on the local database or security server) and uses that information to determine the areas of the network to which the user is allowed access. In AOS, AAA authorization can limit the commands available to a specific user and specify whether or not users can access privileged CLI sessions. Limiting access to privileged CLI sessions is achieved by using the **aaa authorization exec** command to create a default or named method list that restricts access to Enable mode.

Before AAA authorization method lists can be configured or applied, AAA must be enabled. To enable AAA, use the command *aaa on on page 1187*.

Each AAA authorization method list relies on a combination of authorization methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the **group** *<name>* method that can be entered multiple times to accommodate multiple configured server groups. If the unit fails to make a connection with the first group listed, it will try the next group specified.

*For security reasons, Adtran recommends that the **local** authentication method be used instead of the **none** authentication method. Using the **local** authentication method prevents unauthorized users from gaining access to the device during a period in which the links to all authentication servers are down. The local user database contained within the AOS device will always be available and serves as the last line of defense.*

The two types of method lists created using the **aaa authorization exec** command are a default list and a named list. A default list is one that is created and automatically applied to all line interfaces at the global level. A named method list is one that does not perform any action until it is manually applied to an interface. Named AAA exec authorization method lists are applied to line interfaces using the **authorization exec** command from the appropriate line interface configuration mode (*Line (Console) Interface Command Set on page 2021*, *Line (Telnet) Interface Command Set on page 2054*, or *Line (SSH) Interface Command Set on page 2038*).

To use TACACS+ servers to perform Enable mode authorization, the TACACS+ servers must be configured prior to creating the method list. You can configure all TACACS+ servers in the system using the command *tacacs-server on page 1867*. You can configure individual TACACS+ servers using the command *tacacs-server host on page 1868*. Once the TACACS+ servers have been configured, you can use all TACACS+ servers for authorization by using the **group tacacs+** method. If you only want to use some of the available TACACS+ servers for authorization, you can create a named server group and add the TACACS+ servers to the group. Server groups are created using the command *aaa group server on page 1184* and servers are added to the group as outlined in the *TACACS+ Group Command Set on page 4507*.

For more information about AAA authorization, or AAA configuration in general, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates an executive mode authorization method list (called **myList**) to authorize user access to Enable mode in the CLI (this succeeds only if the user has been authenticated successfully):

(config)**#aaa authorization exec myList if-authenticated**

The following example specifies to use the default executive mode authorization method list to authorize access to Enable mode using all TACACS+ servers:

(config)**#aaa authorization exec default group tacacs+**

If a TACACS+ server is used in conjunction with an executive mode access authorization method list, the user name used to access the AOS device must be configured as a Level 15 user on the TACACS+ server.

aaa group server

Use the **aaa group server** command to create a group of remote authentication dial-in user service (RADIUS) servers or a group of terminal access controller access-control system plus (TACACS+) servers. These server groups can be used as methods for authentication, authorization, and accounting (AAA) services in AOS. Use the **no** form of this command to remove a configured server group. Variations of this command include:

aaa group server radius *<group name>*
aaa group server tacacs+ *<group name>*

Syntax Description

radius *<group name>*	Creates and names a group of RADIUS servers.
tacacs+ *<group name>*	Creates and names a group of TACACS+ servers.

Default Values

By default, no named server groups exist.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command was expanded to include TACACS+ server support.

Functional Notes

Server groups can be beneficial when used with AAA method lists because they provide a way to verify AAA services without using all of the configured RADIUS or TACACS+ servers. These server groups are a subset of all RADIUS or TACACS+ servers and can save server resources for other network needs.

Servers must be configured before they can be added to the server group for use with AAA. To configure RADIUS servers on an individual basis, use the command *radius-server host on page 1682*. To configure all RADIUS servers alike, use the command *radius-server on page 1680*. To configure TACACS+ servers on an individual basis, use the command *tacacs-server host on page 1868*. To configure all TACACS+ servers alike, use the command *tacacs-server on page 1867*. It is important to remember when configuring servers for the server group that individual server configurations override any global server configurations.

Once the servers are configured, the **aaa server group** command allows you to begin creating a server group. When you enter the command from the Global Configuration mode prompt, you enter the Server Group Configuration mode. At this point, you can begin to add servers to the group using the **server** command as detailed in the *RADIUS Group Command Set on page 4498* and in the *TACACS+ Group Command Set on page 4507*.

For more information on group server configurations and their use with AAA, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the named list **RADauthentication** and enters the RADIUS Group Configuration mode for RADIUS servers:

(config)**#aaa group server radius RADauthentication**
(config-sg-radius)#

The following example creates the named list **TACaccount** and enters the TACACS+ Group Configuration mode for TACACS+ servers:

(config)**#aaa group server tacacs+ TACaccount**
(config-sg-tacacs+)#

aaa local authentication attempts max-fail <*number*>

Use the **aaa local authentication attempts max-fail** command to set the maximum number of failed authentication attempts allowed before closing the terminal session when using AAA authentication. Use the **no** form of this command to return to the default setting.

Syntax Description

<*number*>	Specifies the maximum number of failed authentication attempts allowed before closing the terminal session. Valid range is **1** to **25** attempts.

Default Values

By default, the session closes after **3** failed attempts.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example configures the device to allow a maximum of **10** failed authentication attempts before closing the session:

(config)**#aaa local authentication attempts max-fail 10**

aaa on

Use the **aaa on** command to activate authentication, authorization, and accounting (AAA) services. Use the **no** form of this command to deactivate AAA.

Syntax Description

No subcommands.

Default Values

By default, AAA is not activated.

Command History

Release 5.1	Command was introduced.

Functional Notes

By default, AAA is disabled. AAA must be enabled for additional AAA configuration commands to be available. If AAA is enabled, AAA methods will override other security methods specified in the line interface.

For more information about the use and configuration of AAA, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example activates AAA services:

(config)**#aaa on**

aaa processes <*value*>

Use the **aaa processes** command to set the number of threads available to the authentication, authorization, and accounting (AAA) background processes. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the number of threads available to the AAA subsystem. Range is **1** to **64** threads.

Default Values

By default, the number of threads is set to **1**.

Command History

Release 5.1	Command was introduced.

Functional Notes

Increasing the number of threads may speed up simultaneous authentication processes, but can do so at the cost of system resources (for example, memory).

For more information about AAA, refer to the *Configuring AAA in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies five available threads for AAA background processes:

(config)**#aaa processes 5**

activchassis deallocate *<vcid>*

Use the **activchassis deallocate** command to delete the entire configuration for a particular device from the ActivChassis configuration.

Syntax Description

<vcid>	Specifies the virtual chassis ID (VCID) of the device to delete from the ActivChassis. Valid range is **1** to **8**. Values 1 and 2 refer to the master and backup device, respectively.

Default Values

No default values are necessary for this command.

Command History

Release AC1.0	Command was introduced.

Functional Notes

The following rules apply to this command:

- The device currently using the specified VCID value must be disconnected and not communicating with the ActivChassis. If the device is connected to ActivChassis, the command is not performed.
- If the device later reconnects to the Activchassis with the same VCID value, it is treated as if it is a new device being added to ActivChassis.
- The VCID cannot be that of the current master.
- Once the command is issued, the device whose VCID has been removed is returned to the linecard default state.

When this command is issued, all configuration corresponding to the device with the specified VCID is deleted from the ActivChassis configuration and the master device's hardware manifest. If the device later reconnects to the ActivChassis with the same VCID value, it is treated as if it is a new device.

The device that has the VCID to be deleted cannot be connected to the ActivChassis when the command is issued. It must be disconnected from the chassis before issuing the command. In addition, deleting the VCID does not change the VCID on the device using that VCID value. You should default the device to clear all ActivChassis information (refer to the command *activchassis restore-linecard-dflt on page 1192*).

Usage Examples

The following example deletes an allocated VCID on a disconnected, non-master device:

(config)**#activchassis deallocate 6**

activchassis front-panel-config

Use the **activchassis front-panel-config** command to enable the ability to configure an ActivChassis ID (VCID) from an ActivChassis device's front panel. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is enabled.

Command History

Release AC1.0	Command was introduced.

Functional Notes

The VCID can always be monitored from a device's front panel.

This command is available from both the ActivChassis master and linecard devices' CLI. For more information about the difference between linecard and master devices, how to access the CLI for each, and additional configuration information, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that front panel configuration of the VCID is disabled for all ActivChassis members:

(config)**#no activchassis front-panel-config**

activchassis renumber *<from vcid> <to vcid>*

Use the **activchassis renumber** command to modify a master-assigned ActivChassis ID (VCID) of an ActivChassis device. This command changes a device's VCID from its current value to a different value. The change is made on the device and in the ActivChassis hardware manifest, but not in the ActivChassis configuration.

Syntax Description

<from vcid>	The current VCID that will be changed on the ActivChassis device. Valid range is **1** to **8** (VCID **1** and **2** refer to the master and backup ActivChassis device, respectively).
<to vcid>	The new VCID to be assigned to the ActivChassis device. Valid range is **1** to **8** (VCID **1** and **2** refer to the master and backup ActivChassis device, respectively).

Default Values

No default values are necessary for this command.

Command History

Release AC1.0	Command was introduced.

Functional Notes

When using this command, remember that the device that currently has the *<from vcid>* value assigned must be connected and actively communicating in the ActivChassis to be renumbered. Neither VCID value can be that of the current master. Master VCID devices must be reassigned by rebooting the device as a standalone unit and then entering the command *activchassis vcid on page 1194*. In addition, the *<to vcid>* value must not be currently allocated. If the value is allocated, you must first deallocate it using the command *activchassis deallocate <vcid> on page 1189*.

If the device with the *<from vcid>* value is present in the ActivChassis, and the VCID values are valid, a warning is displayed indicating that the current VCID and configuration will be changed. You must confirm the changes to be made. Once the changes are confirmed, the VCID of the device is updated to the specified *<to vcid>* value, the master device's manifest is updated with the change, and the targeted device is rebooted for the changes to take effect. The new role and configuration of the new VCID are applied to the device after reboot.

For more information about configuring ActivChassis, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes an allocated VCID (**3**) on a non-master device to VCID **4**:

(config)#**activchassis renumber 3 4**

activchassis restore-linecard-dflt

Use the **activchassis restore-linecard-dflt** command to return an ActivChassis device to the default linecard settings. This command clears the local copy of the ActivChassis manifest, the virtual chassis ID (VCID), and the startup configuration for the device. This command is most useful when a device that was connected to an ActivChassis needs to be restored to the factory settings or have all knowledge of its existence in the virtual chassis removed.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release AC1.0	Command was introduced.

Functional Notes

This command is available from both the ActivChassis master and linecard devices' CLI. For more information about the difference between linecard and master devices, how to access the CLI for each, and additional configuration information, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example defaults a non-linecard (master or backup) ActivChassis device:

(config)**#activchassis restore-linecard-dflt**

activchassis strict-firmware

Use the **activchassis strict-firmware** command to prevent linecard devices from joining an ActivChassis when their firmware image differs from that of the master device. Use the **no** form of this command to allow linecard devices with different firmware images to join the chassis.

Syntax Description

No subcommands.

Default Values

By default, linecard devices with different firmware images are allowed to join the ActivChassis.

Command History

Release AC1.0	Command was introduced.

Functional Notes

When linecard devices have mismatched firmware, Activchassis displays a warning message every 30 seconds that states which linecard has the improper firmware.

For more information about configuring ActivChassis, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that all linecard devices must have the same firmware image as the master device before they can join the ActivChassis:

(config)**#activchassis strict-firmware**

activchassis vcid

Use the **activchassis vcid** command to create an ActivChassis master device or specify a local standalone device as a member of the ActivChassis and to specify the virtual chassis ID (VCID). Use the **no** version of this command to disable the ability to configure the VCID on the local device. Variations of this command include:

activchassis vcid master-assigned
activchassis vcid <*value*>

Syntax Description

master-assigned	Specifies that the VCID is assigned by the master device when a standalone device is admitted to the ActivChassis.
<*value*>	Specifies the VCID as a value between **1** and **8**. Values **1** and **2** are used to specify a master and backup device, respectively.

Default Values

By default, when a standalone device joins the ActivChassis the VCID is **master-assigned**.

Command History

Release AC1.0	Command was introduced.

Functional Notes

Once this command is entered, you are asked to confirm that the device configuration and operating mode will be altered. After confirmation, if the device is currently ActivChassis disabled, it becomes ActivChassis enabled, and the file system is updated with the VCID. If the device has already been ActivChassis enabled, the VCID is changed to the specified value. In either case, the device reboots, and any unconfigured ActivChassis capable ports on the device default to ActivChassis mode.

If the command is entered on a device that is already ActivChassis enabled, and the VCID specified is the same as the VCID currently in use, it will have no effect and the command will not be performed.

This command is available from both the ActivChassis master and linecard devices' CLI. For more information about the difference between linecard and master devices, how to access the CLI for each, and additional configuration information, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables ActivChassis and specifies the VCID of the device:

(config)**#activchassis vcid 3**

arp <*ip address*> <*mac address*> arpa

Use the **arp arpa** command to enter static entries into the Address Resolution Protocol (ARP) table for a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove a static ARP entry. Variations of this command include:

arp <*ip address*> <*mac address*> **arpa**
arp <*ip address*> <*mac address*> **vrf** <*name*> **arpa**

Syntax Description

<*ip address*>	Specifies a valid IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*mac address*>	Specifies a valid 48-bit medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
vrf <*name*>	Optional. Specifies the VRF where the ARP table exists.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example enters the IP address and MAC address into the ARP table that is located in the default VRF:

(config)**#arp 10.10.10.1 00:A0:C8:00:00:01 arpa**

as-path-list *<name>*

Use the **as-path-list** command to create IP autonomous system (AS) path lists for route map use. Use the **no** form of this command to delete the AS path list.

Syntax Description

<name>	Specifies the name of the AS path list. Refer to *AS Path List Command Set on page 3978* for more information on the available options.

Default Values

By default, no AS path lists are defined.

Command History

Release 9.3	Command was introduced.
Release R10.1.0	The **ip** keyword was removed from this command.

Functional Notes

AS path lists are a type of route filter that permits or denies Border Gateway Protocol (BGP) routes based on the AS_PATH attribute. AS path lists define a list of AS specifications that, once created, may then be referenced in a route map. Refer to the *Usage Examples* section below.

Usage Examples

The following example creates the AS path list **list5** and enters the IP **as-path-list** command mode:

```
(config)#as-path-list list5
(config-as-path-list)#
```


auto-config

Use the **auto-config** command to enable and start the AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Use the **no** form of this command to halt the automatic configuration process.

*Disabling using the **no auto-config** command and re-enabling using the **auto-config** command, restarts the download process.*

Syntax Description

No subcommands.

Default Values

By default, **auto-config** is enabled on the Total Access 900(e) Series, NetVanta 644, NetVanta 1335, NetVanta 3000 Series, NetVanta 4000 Series, NetVanta 5000 Series, and NetVanta 6000 Series products. By default, **auto-config** is disabled on all other products not specified above.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables automatic configuration:

(config)**#auto-config**

auto-config apply-config

Use the **auto-config apply-config** command to specify the preferred method of applying the AOS automatic self-configuration settings to the running configuration. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Variations of this command include:

auto-config apply-config append
auto-config apply-config replace

Syntax Description

append	Appends the automatic self-configuration parameters to the end of the current running configuration and retains the existing running configuration. It does not save this information to the startup configuration. Refer to the *Functional Notes* below for more information.
replace	Replaces the startup configuration. This parameter erases all current configuration information and saves to the startup configuration.

Default Values

By default, the configuration is set to **append**.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

Using the **append** keyword only appends the parameters to the currently running configuration. The appended parameters will not be retained if the unit is rebooted. To permanently store the appended configuration settings, you must save the running configuration as the startup configuration by issuing the **do write** command. This can be performed manually, after the append process is complete, or added as the final line in the self-configuration parameters to automatically save after appending.

Usage Examples

The following example overwrites the startup configuration:

(config)**#auto-config apply-config replace**

The following example adds the configuration parameters to the running configuration:

(config)**#auto-config apply-config append**

auto-config authname <*username*> password <*password*>

Use the **auto-config authname password** command to specify the user name and password to use for authentication with the AOS automatic self-configuration feature. If authentication is required for Trivial File Transfer Protocol (TFTP), Hypertext Transfer Protocol (HTTP), and Hypertext Transfer Protocol Secure (HTTPS), the user name and password must be resolved before the file transfer can commence. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com.

Syntax Description

authname <*authname*>	Enter the authentication user name or define a system variable using parameters representing one of the following system values: $SYSTEM_NAME - the host name of the system $SYSTEM_SERIAL_NUMBER - the serial number of the system $SYSTEM_DESCRIPTION - the product name and software version $SYSTEM_SOFTWARE_VERSION - the running software version $AUTH_MAC_ADDRESS - MAC address for MAC authentication
password <*password*>	Specifies the authentication password.

Default Values

By default, this setting is disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example specifies the Auto-Config authentication user name as the system serial number and specifies the password to use:

(config)**#auto-config authname $SYSTEM_SERIAL_NUMBER password fRiax&crOus9l#p**

auto-config filename

Use the **auto-config filename** command to specify the file name to download for the AOS automatic self-configuration feature. The file name can be defined as a static file name or defined using parameters representing system values. A static file name can include a partial path. The file name can also be defined using Dynamic Host Configuration Protocol (DHCP) Option 67. Use the **no** form of this command to erase the stored file name. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Variations of this command include:

auto-config filename <*name*>
auto-config filename dhcp

Syntax Description

filename dhcp	Specifies the configuration file name is provided through DHCP Option 67.
filename <*name*>	Specify the configuration file name or define a system parameter using variables. Including the file path in addition to the file name or variable is optional. The following variables are allowed to represent system values: $SYSTEM_NAME - host name of the system $SYSTEM_SERIAL_NUMBER - serial number of the system $SYSTEM_DESCRIPTION - product name and software version $SYSTEM_SOFTWARE_VERSION - running software's version $AUTH_MAC_ADDRESS - MAC address used for MAC authentication

Default Values

By default, the file name uses DHCP Option 67 to retrieve the file name.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was expanded to include parameter **dhcp** for DHCP Option 67.

Functional Notes

If no file name is specified, Auto-Config attempts to locate additional configuration files on the server device as a fallback measure. The configuration file names searched for in such a situation include (in order of priority): a file name based on MAC addresses (<*MAC#1*>**.cfg**), a file name based on the AOS device part number (**adtran_**<*Unit Part Number*>**.cfg**), and the Adtran default file name (**adtran_000000000000.cfg**).

Usage Examples

The following command specifies a static file name to download:

(config)**#auto-config filename AUTO_CONFIG.cfg**

The following command specifies a static file name and includes a path to the file:

(config)**#auto-config filename config/adtran/AUTO_CONFIG.cfg**

The following command configures the unit to retrieve the file name according to the DHCP Option 67:

(config)**#auto-config filename dhcp**

The following command specifies the file name using the system variable SYSTEM NAME:

(config)**#auto-config filename $SYSTEM_NAME.cfg**

The following command specifies the file name using the system variable SYSTEM NAME and includes the file path:

(config)**#auto-config filename config/adtran/$SYSTEM_NAME.cfg**

auto-config firmware

Use the **auto-config firmware** command to enable and configure firmware download for the AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com.Variations of this command include:

auto-config firmware definition-file <*name*>
auto-config firmware destination cflash
auto-config firmware destination flash
auto-config firmware download
auto-config firmware reload-after <*seconds*>
auto-config firmware replace primary maintain secondary
auto-config firmware replace primary update secondary
auto-config firmware replace secondary

Syntax Description

definition-file <*name*>	Specifies the path and static file name of the definition file.
destination	Specifies where to store the downloaded firmware image.
cflash	Specifies to store the downloaded firmware image on the unit's CompactFlash memory.
flash	Specifies to store the downloaded firmware image on the unit's flash memory.
download	Enables the firmware download.
reload-after <*seconds*>	Specifies the delay, in seconds,after downloading the new firmware image before the unit reboots. The valid range is **60** through **604800**. Use the value **0** to disable the reboot.
replace primary	Specifies to replace the current primary firmware image with the new image.
maintain secondary	Specifies to retain the existing secondary firmware image, if one exists, and delete the current primary image.
update secondary	Specifies that the existing primary firmware image becomes the new secondary image, and deletes the existing secondary image.
replace secondary	Specifies to replace the existing secondary firmware image with the new image, deleting the existing secondary image, while retaining the current primary image.

Default Values

By default, this feature is disabled. When enabled, the default file system is **flash** unless otherwise specified.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example specifies the name and location and name of the definition file:

(config)**#auto-config firmware definition-file config/adtran/myconfig.biz**

The following example specifies the download location as the CompactFlash memory:

(config)**#auto-config firmware destination cflash**

auto-config http-auth

Use the **auto-config http-auth** command to configure the Hypertext Transfer Protocol (HTTP) authentication mode for the AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Use the **no** form of this command to disable the specified mode. Each mode can be turned on or off individually. Variations of this command include:

auto-config http-auth basic
auto-config http-auth digest

> NOTE *At least one mode must be enabled at all times. An error message will occur if an attempt is made to disable both authentication modes.*

Syntax Description

basic	Enables the HTTP(S) basic authentication mode, using clear text authentication.
digest	Enables the HTTP(S) digest authentication mode, using encrypted text authentication.

Default Values

By default, both **basic** and **digest** modes are enabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example enables the basic HTTP authentication mode:

(config)**#auto-config http-auth basic**

The following example disables the digest HTTP authentication mode:

(config)**#no auto-config http-auth digest**

auto-config mac-auth

Use the **auto-config mac-auth** command to configure medium access control (MAC) address authentication for the AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Variations of this command include:

auto-config mac-auth address <*mac address*>
auto-config mac-auth interface <*interface*>
auto-config mac-auth mode http-user-agent
auto-config mac-auth mode none

Syntax Description

address <*mac address*>	Specifies the 48-bit MAC address to use for authentication. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**). For this command, colons are optional.
interface <*interface*>	Specifies an interface from which to use the MAC address for authentication. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet interface, use **eth 0/1**, for an Ethernet subinterface, use **eth 0/1.1**. Type **auto-config mac-auth interface ?** for a complete list of valid interfaces.
mode	Specifies the MAC authentication mode to use.
http-user-agent	Specifies including the MAC address in the HTTP User Agent header.
none	Specifies not to include the MAC address in the HTTP User Agent header.

Default Values

By default, MAC authentication is disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example enables **http-user-agent** mode and specifies the MAC address **00:A0:C8:00:00:01** for authentication:

(config)**#auto-config mac-auth mode http-user-agent**
(config)**#auto-config mac-auth address 00:A0:C8:00:00:01**

The following example enables **http-user-agent** mode and specifies using the MAC address assigned to the Ethernet 0/1 interface for authentication:

(config)**#auto-config mac-auth mode http-user-agent**
(config)**#auto-config mac-auth interface ethernet 0/1**

The following example disables MAC address authentication:

(config)**#auto-config mac-auth mode none**

auto-config method

Use the **auto-config method** command to configure the file transfer method to use during AOS automatic self-configuration. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Variations of this command include:

auto-config method http
auto-config method http port <*number*>
auto-config method https
auto-config method https allow-tls1.0
auto-config method https allow-tls1.0 allow-tls1.1
auto-config method https allow-tls1.0 allow-tls1.1 allow-sslv3
auto-config method https allow-tls1.0 allow-sslv3
auto-config method https allow-tls1.1
auto-config method https allow-tls1.1 allow-sslv3
auto-config method https allow-sslv3
auto-config method https port <*number*>
auto-config method https port <*number*> **allow-tls1.0**
auto-config method https port <*number*> **allow-tls1.0 allow-tls1.1**
auto-config method https port <*number*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
auto-config method https port <*number*> **allow-tls1.0 allow-sslv3**
auto-config method https port <*number*> **allow-tls1.1**
auto-config method https port <*number*> **allow-tls1.1 allow-sslv3**
auto-config method https port <*number*> **allow-sslv3**
auto-config method tftp

Syntax Description

http	Specifies using Hypertext Transfer Protocol (HTTP) for the file transfer method.
https	Specifies using Hypertext Transfer Protocol Secure (HTTPS) for the file transfer method.
allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS protocol version 1.1 if **allow-tls1.1** is enabled. SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3. If SSLv3 is enabled, TLS version 1.0 is automatically enabled.
port <*number*>	Optional. Specifies the port number to use for the HTTP(S) file transfer method. The valid range is **1** through **65535**. If a specific port number is not entered, the default port number is used.
tftp	Specifies using Trivial File Transfer Protocol (TFTP) for the file transfer method.

Default Values

By default, the file transfer method is TFTP. If specifying HTTP, the default port is 80. If specifying HTTPS, the default port is 443.

Command History

Release R10.5.0	Command was introduced.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example enables TFTP as the file transfer method for automatic configuration:

(config)**#auto-config method tftp**

The following example enables HTTPS as the file transfer method and uses the default HTTPS port of **443**:

(config)**#auto-config method https**

The following example enables HTTPS as the file transfer method, and specifies using the port number **6335**:

(config)#auto-config method https port **6335**

auto-config retry-count *<number>*

Use the **auto-config retry-count** command to specify the maximum number of retries allowed to download a configuration file through AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Use the **no** form of this command to return to the default number of retries.

Syntax Description

<number>	Specify the maximum number of attempts allowed. Valid range is **0** to **1000**.

Default Values

By default, the number of retries is set to **0** allowing the feature to continuously retry until the feature is disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following command sets the number of retries when downloading a configuration file to **100**:

(config)**#auto-config retry-count 100**

auto-config server

Use the **auto-config server** command to specify the Trivial File Transfer Protocol (TFTP) or Dynamic Host Configuration Protocol (DHCP) server to use during automatic self-configuration. The TFTP or DHCP server provides the configuration file necessary for automatic self-configuration. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Use the **no** form of this command to erase the stored server name. Variations of this command include:

auto-config server [<*hostname*> **|** <*ipv4 address*>**]**
auto-config server dhcp
auto-config server dhcp option [66 | **160]**

Syntax Description

server dhcp	Specifies using DHCP Option 66 to locate the server.
server dhcp option 66	Optional. Specifies using Option 66 to locate the server.
server dhcp option 160	Optional. Specifies using Option 160 to locate the server.
server [<*hostname*> **|** <*ipv4 address*>**]**	Specifies the IPv4 address or host name of TFTP server. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, Auto-Config attempts to locate the server using DHCP Option 66.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was expanded to include **dhcp**, **dhcp option 66**, and **dhcp option 160** parameters.

Usage Examples

The following command specifies the TFTP server IPv4 address from which to download the configuration file:

(config)**#auto-config server 192.33.5.99**

The following command specifies the TFTP server host name from which to download the configuration file:

(config)**#auto-config server MYHOST**

The following command specifies using DHCP Option 66 to locate the DHCP server from which to download the configuration file:

(config)**#auto-config server dhcp 66**

auto-config sip-notify reboot

Use the **auto-config sip-notify reboot** command to specify the units reboot behavior when receiving a SIP NOTIFY. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com.Variations of this command include:

auto-config sip-notify reboot always
auto-config sip-notify reboot on-change

Syntax Description

always	Specifies that the unit reboot regardless of the configuration.
on-change	Specifies that the unit reboot only if the configuration on the server has changed.

Default Values

By default, the reboot behavior when receiving a SIP NOTIFY is **on-change**.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example specifies that the unit reboot regardless of the configuration when receiving a SIP NOTIFY:

(config)**#auto-config sip-notify reboot always**

auto-config sip-notify user <*user*>

Use the **auto-config sip-notify user** command to enable and configure a Session Initiation Protocol (SIP) user to receive check-sync events to initiate the AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com. Use the **no** form of this command to halt the automatic configuration process.

> NOTE *Only certain AOS devices support SIP NOTIFY check-sync events. In order for the SIP NOTIFY message to be received, the AOS platform must support **sip** (this excludes switches and routers without SIP proxy), and have it enabled in the configuration. The firewall must be provisioned to allow the unit to receive SIP messages from the server.*

Syntax Description

<*user*>	Specifies the SIP user to which the NOTIFY (check-sync event) is sent.

Default Values

By default, this feature is disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example enables the SIP user **2001** to receive the SIP NOTIFY (check-sync event):

(config)**#auto-config sip-notify user 2001**

auto-config timer polling <*seconds*>

Use the **auto-config timer polling** command to periodically restart the AOS automatic self-configuration feature. For more detailed information, refer to the *Configuring Auto-Config* guide available online at https://supportcommunity.adtran.com.

Syntax Description

<*seconds*>	Specifies the restart interval in seconds. The valid range is **30** to **2592000**.

Default Values

By default, this feature is disabled.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example sets the restart interval to **320** seconds:

(config)**#auto-config timer polling 320**

auto-link

Use the **auto-link** command to enable the auto-link feature, to specify the communication method between an AOS device and the n-Command® managed service provider (MSP) server, and to optionally specify the service name prefix of service (SRV) record requests. Communication can be either via Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Auto-link allows a client device to connect to an Adtran n-Command MSP network management appliance. Use the **no** form of this command to disable auto-link or to return to the default communication method. Variations of this command include:

auto-link
auto-link http
auto-link http srv <*prefix*>
auto-link https
auto-link https allow-tls1.0
auto-link https allow-tls1.1
auto-link https srv <*prefix*>
auto-link https allow-tls1.0 srv <*prefix*>
auto-link https allow-tls1.1 srv <*prefix*>

Syntax Description

http	Optional. Specifies that the client use the HTTP posting method.
https	Optional. Specifies that the client use the HTTPS posting method.
allow-tls1.0	Optional. Enables support for Transport Layer Security (TLS) protocol version 1.0.
allow-tls1.1	Optional. Enables support for TLS protocol version 1.1.
srv <*prefix*>	Optional. Specifies the service name prefix of SRV requests.

Default Values

By default, auto-link is disabled. By default, auto-link uses **HTTPS**. By default, if no service name prefix is configured, auto-link uses **_http** for HTTP communication, and **_https** for HTTPS communication. By default, support for TLS version 1.0 is disabled.

Command History

Release 17.3/A1	Command was introduced.
Release R10.7.0	Command was expanded to include the **srv** <*prefix*> parameter.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** parameter.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Functional Notes

The n-Command client must first be configured and enabled before the n-Command MSP server can be contacted. The n-Command MSP server is a network management appliance that enables auto-discovery of the AOS unit and provides a central management solution for configuration changes, firmware updates, and basic monitoring. Without enabling auto-link, the client will not be detected by the server. For more information about configuring the auto-link feature, refer to the configuration guide *Configuring Auto-Link for AOS and n-Command MSP* available online at https://supportcommunity.adtran.com.

The service name prefix, such as **_http**, can be any arbitrary string, but the protocol prefix is **_tcp** for auto-link. Do not include the leading underscore for service name prefixes. The underscore is added automatically.

TLS versions 1.0 and 1.1 can no longer be used as a security control due to their weakness as cryptography methods. By default, TLS version 1.0 and 1.1 are disabled for auto-link configurations.

Usage Examples

The following example enables auto-link:

(config)**#auto-link**

The following example specifies that the client use HTTP to communicate with the server:

(config)**#auto-link http**

auto-link penalty *<value>*

Use the **auto-link penalty** command to enable and configure a temporary penalty list for auto-link configuration. The temporary penalty list blacklists hosts that cause repeated communication failures. If a server of configured IP address causes a failover event three consecutive times, it is added to the penalty list. Once added to the list, auto-link will not contact the server for a configured number of recontact intervals. Using the **no** form of this command removes the penalty list from the auto-link configuration.

Syntax Description

<value>	Specifies the number of recontact intervals that the server will stay on the penalty list. Valid range is **0** to **65535**. Using a value of **0** disables the penalty feature.

Default Values

By default, the penalty feature is disabled.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Penalty lists can be based on IP addresses and port numbers. Host IP addresses and port numbers returned from DNS requests, as well as configured IP addresses and port numbers, can be penalized.

Usage Examples

The following example enables recontact interval penalties and specifies that penalized servers remain on the list for **30** recontact intervals:

(config)**#auto-link penalty 30**

auto-link recontact-interval *<value>*

Use the **auto-link recontact-interval** command to specify the intervals between contact attempts between the AOS client and the n-Command® managed service provider (MSP) server. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the time in seconds between contact attempts. Range is **20** to **604800** seconds. Setting this value to **0** seconds disables the recontact feature.

Default Values

By default, the recontact interval is set to **3600** seconds.

Command History

Release 17.3/A1	Command was introduced.

Usage Examples

The following example sets the recontact interval to **7200** seconds:

(config)**#auto-link recontact-interval 7200**

auto-link region *<region name>*

Use the **auto-link region** command to assign a region name to an AOS device associated with the n-Command® managed service provider (MSP) server. Use the **no** form of this command to remove the region name from the AOS device's configuration.

Syntax Description

<region name>	Specifies the name of the region associated with the AOS device. Specify the region name in a text string.

Default Values

By default, a region name is not specified.

Command History

Release R13.1.0	Command was introduced.

Functional Notes

Regions are used in n-Command® MSP to allow network administrators to limit a specific user's access to devices. For user regions to work properly, the AOS device must be assigned a region name, a region must be created in n-Command® MSP with a filter value that matches all or part of the created AOS device's region name, and the region must be assigned to a user.

Usage Examples

The following example sets the region name for the AOS device:

(config)**#auto-link region REGIONONELOCAL**

auto-link server <*hostname* | *ip address*>

Use the **auto-link server** command to specify the contact information for the n-Command® managed service provider (MSP) server used by the AOS client. Use the **no** form of this command to remove the server from the client configuration. Variations of this command include:

auto-link server primary <*hostname* | *ip address*>
auto-link server primary <*hostname* | *ip address*> **port** <*port*>
auto-link server secondary <*hostname* | *ip address*>
auto-link server secondary <*hostname* | *ip address*> **port** <*port*>

Syntax Description

primary	Specifies the primary auto-link server. The primary server must be specified. Only one entry is allowed for the primary server.
secondary	Specifies the secondary auto-link server. Secondary servers are used in auto-link failover situations where the primary server is unavailable. Multiple secondary servers can be configured. The priority of secondary servers is determined by the order in which the servers are configured.
<*hostname* | *ip address*>	Specifies the server host name or IP address. IP addresses should be expressed in the decimal dotted notation (for example **10.10.10.1**).
port <*port*>	Optional. Specifies the port number used to communicate with the server. Valid range is **1** to **65535**.

Default Values

By default, no server is configured. When specified, the server uses port **80** for Hypertext Transfer Protocol (HTTP) and port **443** for HTTP secure (HTTPS).

Command History

Release 17.3/A1	Command was introduced.
Release R10.7.0	Command was expanded to include options to specify **primary** and **secondary** servers.

Functional Notes

The host name or the IP address of the server with which the AOS product communicates must be specified for communication to take place. A primary server must be specified, and secondary servers can optionally be configured. Only one entry is allowed for the primary MSP server. To delete the primary MSP server, you must first remove all configured secondary servers.

Usage Examples

The following example specifies the AOS client will communicate with the primary n-Command MSP server at IP address **10.10.10.10**:

(config)**#auto-link server primary 10.10.10.10**

auto-link vrf *<name>*

Use the **auto-link vrf** command to specify the virtual routing and forwarding (VRF) instance on which auto-link will communicate. Use the **no** form of this command to return to the default value.

Syntax Description

<name>	Specifies the name of the VRF on which auto-link will operate.

Default Values

By default, auto-link is configured to operate on the default (unnamed) VRF.

Command History

Release R11.12.0	Command was introduced.

Functional Notes

All auto-link messages, such as information status messages and backup file uploads, are transmitted on the default VRF. When a domain name is specified as the auto-link server, the domain name system (DNS) operation also occurs on the specified VRF.

This command is configured separate from the command *auto-link on page 1214*, which enables/disables the auto-link feature.

If a specified VRF does not exist, an error is returned.

When a nondefault VRF is configured for auto-link, the VRF is displayed in the output of the command *show auto-link on page 557*. If auto-link is configured to operate on the default VRF, then the VRF information is not displayed in the **show** command output.

Usage Examples

The following example configured auto-link to use the nondefault VRF **RED**:

(config)**#auto-link vrf RED**

banner

Use the **banner** command to specify messages to be displayed in certain situations. Use the **no** form of this command to delete a previously configured banner. Variations of this command include:

banner exec *<delimiter> <message> <delimiter>*
banner login *<delimiter> <message> <delimiter>*
banner motd *<delimiter> <message> <delimiter>*

Syntax Description

exec	Creates a message to be displayed when any executive-level process takes place.
login	Creates a message to be displayed before the user name and password login prompts.
motd	Creates a message-of-the-day (MOTD) banner.
<delimiter>	Specifies the banner text delimiter. Press **Enter** after the delimiter character to begin input of banner text. After typing the banner message, enter the same delimiter character to end the message.
<message>	Specifies the text message you wish to display.

Default Values

By default, no banners are configured.

Command History

Release 2.1	Command was introduced.

Functional Notes

Banners appear in the following order (if configured):

- MOTD banner appears at initial connection.
- Login banner follows the MOTD banner.
- Exec banner appears after successful login.

Usage Examples

The following example configures the system to display a message of the day:

(config)**#banner motd *The system will be shut down today from 7PM to 11PM***

battery <*slot/port*>

Use the **battery** <*slot/port*> command to enter the Battery Configuration mode for the specified slot and port, in order to configure the battery installation time and date.

Additional subcommands are available once you have entered the Battery Configuration mode. Use the **no** form of the **install date set** commands to clear the settings. Variations of the commands include:

install date set <*time*> <*date*>
install date set clock

Syntax Description

<*slot/port*>	Specifies the slot and port of the battery.
install date set <*time*> <*date*>	Specifies a time and date for when the battery is installed. Enter the <*time*> value in the HH:MM:SS format. Enter the <*date*> value in the DD Month YYYY format.
install date set clock	Specifies the battery install date and time is set using the system clock if the system clock has been set either manually or from NTP.

Default Values

By default, no battery install time and date exists.

Command History

Release R11.10.0	Command was introduced.
Release R11.11.0	Command was expanded to include the **clock** parameter.

Usage Examples

The following example enters the Battery Configuration mode for slot **0**, port **1** and sets the install time to **12:30:22** and date to **4 June 2015**:

(config)**#battery 0/1**
(config-battery 0/1)**#install date set 12:30:22 4 June 2015**
(config-battery 0/1)**#exit**
(config)**#**

boot config

Use the **boot config** command to modify system boot parameters by specifying the location and name of primary and secondary configuration files. Use the **no** form of this command to use the default startup configuration file. Variations of this command include:

boot config cflash <*primary filename*>
boot config cflash <*primary filename*> **cflash** <*secondary filename*>
boot config cflash <*primary filename*> **flash** <*secondary filename*>
boot config flash <*primary filename*>
boot config flash <*primary filename*> **cflash** <*secondary filename*>
boot config flash <*primary filename*> **flash** <*secondary filename*>
boot config flash <*primary filename*> **usbdrive0** <*secondary filename*>
boot config usbdrive0 <*primary filename*>
boot config usbdrive0 <*primary filename*> **flash** <*secondary filename*>
boot config usbdrive0 <*primary filename*> **usbdrive0** <*secondary filename*>

NOTE *The **cflash** parameter is only valid for units with CompactFlash® capabilities.*

NOTE *The **usbdrive0** parameter is only valid for units with Universal Serial Bus (USB) flash drive capabilities.*

Syntax Description

cflash	Specifies that the configuration file is located in CompactFlash memory.
flash	Specifies that the configuration file is located in flash memory.
usbdrive0	Specifies that the configuration file is located in USB flash drive memory.
<*primary filename*>	Specifies the name of the primary configuration file (file names are case sensitive).
<*secondary filename*>	Optional. Specifies the name of the backup configuration file.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 18.2	Command was expanded to include USB flash drive memory.

Usage Examples

The following example specifies the file **myconfig.biz** (located in flash memory) as the primary system boot file:

(config)**#boot config flash myconfig.biz**

The following example specifies the file **myconfig.biz** (located in flash memory) as the primary system boot file and the file **mybackupconfig.biz** (located in CompactFlash memory) as the backup configuration file:

(config)**#boot config flash myconfig.biz cflash mybackupconfig.biz**

boot system

Use the **boot system** command to specify the system image loaded at startup. Variations of this command include:

boot system cflash <*primary filename*>
boot system cflash <*primary filename*> **verify**
boot system cflash <*primary filename*> **cflash** <*secondary filename*>
boot system cflash <*primary filename*> **cflash** <*secondary filename*> **verify**
boot system cflash <*primary filename*> **flash** <*secondary filename*>
boot system cflash <*primary filename*> **flash** <*secondary filename*> **verify**
boot system cflash <*primary filename*> **no-backup**
boot system cflash <*primary filename*> **no-backup verify**
boot system flash <*primary filename*>
boot system flash <*primary filename*> **verify**
boot system flash <*primary filename*> <*secondary filename*>
boot system flash <*primary filename*> <*secondary filename*> **verify**
boot system flash <*primary filename*> **cflash** <*secondary filename*>
boot system flash <*primary filename*> **cflash** <*secondary filename*> **verify**
boot system flash <*primary filename*> **flash** <*secondary filename*>
boot system flash <*primary filename*> **flash** <*secondary filename*> **verify**
boot system flash <*primary filename*> **no-backup**
boot system flash <*primary filename*> **no-backup verify**
boot system flash <*primary filename*> **usbdrive0** <*secondary filename*>
boot system flash <*primary filename*> **usbdrive0** <*secondary filename*> **verify**
boot system usbdrive0 <*primary filename*>
boot system usbdrive0 <*primary filename*> **verify**
boot system usbdrive0 <*primary filename*> **flash** <*secondary filename*>
boot system usbdrive0 <*primary filename*> **flash** <*secondary filename*> **verify**
boot system usbdrive0 <*primary filename*> **no-backup**
boot system usbdrive0 <*primary filename*> **no-backup verify**
boot system usbdrive0 <*primary filename*> **usbdrive0** <*secondary filename*>
boot system usbdrive0 <*primary filename*> **usbdrive0** <*secondary filename*> **verify**

*The **cflash** parameter is only valid for units with CompactFlash® capabilities.*

*For units without CompactFlash capabilities, the secondary media type does not need to be specified. Refer to the last example under **Usage Examples**.*

*The **usbdrive0** parameter is only valid for units with Universal Serial Bus (USB) flash drive capabilities.*

Syntax Description

cflash	Specifies the system image is located in CompactFlash memory.
flash	Specifies the system image is located in flash memory.
no-backup	Specifies that there is no backup image present.
<primary filename>	Specifies the file name of the image (file names are case sensitive). Image files should have a .biz extension.
<secondary filename>	Specifies a name for the backup image.
verify	Optional. Verifies the image checksum.
usbdrive0	Specifies the system image is located in USB flash drive memory.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 12.1	Command was expanded to include CompactFlash.
Release 18.2	Command was expanded to include USB flash drive memory.
Release R12.1.0	Command version **boot system flash** was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

Detailed instructions for upgrading AOS and loading files into flash memory are found online at http://supportforums.adtran.com.

The **boot system flash** command is not available in vAOS instances.

Usage Examples

The following example specifies **myimage.biz** (located in CompactFlash memory) as the primary image file with no backup image:

(config)**#boot system cflash myimage.biz no-backup**

The following example specifies **myimage.biz** (located in flash memory) as the primary image file with no backup image:

(config)**#boot system flash myimage.biz no-backup**

The following example specifies **myimage.biz** (located in flash memory) as the primary image file and **mybackupimage.biz** (also located in flash memory) as the backup image:

(config)#**boot system flash myimage.biz mybackupimage.biz**

boot voip

Use the **boot voip** command to specify the VoIP image file loaded at startup. Variations of this command include:

boot voip default
boot voip flash <*filename*>

Syntax Description

default	Uses default VoIP image.
flash <*filename*>	Specifies the file name (located in flash memory) of the image (file names are case sensitive). Image files should have a .biz extension.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

Detailed instructions for upgrading AOS and loading files into flash memory are found online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the file **myimage.biz**, stored in flash memory, as the VoIP startup image:

(config)**#boot voip flash myimage.biz**

bridge irb

Use the **bridge irb** command to enable integrated routing and bridging (IRB) and also allow the creation of bridged virtual interfaces (BVIs). Use the **no** form of this command to disable the IRB.

Syntax Description

No subcommands.

Default Values

By default, IRB is disabled.

Command History

Release 15.1	Command was introduced.

Functional Notes

The **bridge irb** *must* be enabled to create BVIs.

Once the command **bridge irb** is entered, the IP addresses for any interfaces connected to *any* bridge will be removed. Also, the command **ip address xx.xx.xx.xx.xx.xx.xx.xx** will no longer be available on an interface that is connected to the bridge.

The BVI must be removed before using the **no bridge irb** command.

For more information on BVI configuration, refer to the *BVI Interface Command Set on page 2593*.

Usage Examples

The following example enables IRB:

(config)**#bridge irb**

Technology Review

The IRB allows the routing of specified protocols between network interfaces and bridge groups. The difference between IRB and concurrent routing and bridging (CRB) is that in IRB it is possible to route IP between routed interfaces and BVIs, but with CRB the routed interfaces cannot communicate with bridged interfaces. IRB's primary goal is to bridge all protocols and route any IP traffic destined for the medium access control (MAC) address of the BVI.

The IRB handles IP packets in the following manner: When an IP packet comes into the router and it is not destined for the MAC address, it is bridged. If the IP packet is destined for the MAC address, it is sent to the routing engine and routed as normal. The IRB allows for PCs in the bridge to get to routed networks and routed networks to get to the bridge. The bridge group will isolate broadcasts from other routed interfaces.

A BVI can only be created when IRB is enabled and a bridge group has been defined. The BVI number corresponds directly to the bridge group.

When IRB *is* enabled and a BVI is configured, IP network configuration is removed for all bridged interfaces. IP traffic destined for the BVI address is delivered to the local IP stack for routing (if routing is enabled) or management. If no BVI is configured, the behavior is the same as if IRB is not enabled.

When IRB is *not* enabled, a BVI cannot be created. Bridged interfaces retain their IP configuration, and IP traffic destined for those interfaces is delivered to the local IP stack.

bridge <*number*> protocol ieee

The **bridge protocol ieee** command configures a bridge group for the IEEE 802.1 Ethernet spanning-tree protocol. Use the **no** form of this command (with the appropriate arguments) to delete this setting.

Syntax Description

<*number*>	Specifies a bridge group number. Range is **1** to **255**.

Default Values

By default, all configured bridge interfaces implement IEEE spanning-tree protocol.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example deletes the bridge protocol setting for bridge group **17**:

(config)**#no bridge 17 protocol ieee**

clock

The **clock auto-correct-DST** command allows the unit to automatically correct for daylight savings time (DST). Use the **clock no-auto-correct-DST** command to disable this feature. Variations of this command include:

clock auto-correct-DST
clock no-auto-correct-DST

Syntax Description

auto-correct-DST	Configures the unit to automatically correct for DST.
no-auto-correct-DST	Disables DST correction.

Default Values

By default, DST correction takes place automatically.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was added to the Global command set.

Functional Notes

Depending on the **clock timezone** chosen (refer to *clock timezone <value> on page 1234* for more information), one-hour DST correction may be enabled automatically. You may override this default using this command.

Usage Examples

The following example allows for automatic DST correction:

(config)**#clock auto-correct-DST**

The following example overrides the one-hour offset for DST:

(config)**#clock no-auto-correct-DST**

clock set *<time> <day> <month> <year>*

Use the **clock set** command to configure the system software clock. For the command to be valid, all fields must be entered. Refer to the *Usage Examples* below for an example.

Syntax Description

<time>	Sets the time (in 24-hour format) of the system software clock in the format hours:minutes:seconds (HH:MM:SS).
<day>	Sets the current day of the month. Valid range is **1** to **31**.
<month>	Sets the current month. Valid range is **January** to **December**. You need only enter enough characters to make the entry unique. This entry is not case sensitive.
<year>	Sets the current year. Valid range is **2000** to **2100**.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was added to the Global command set.

Usage Examples

The following example sets the system software clock for 3:42 pm, August 22 2004:

(config)**#clock set 15:42:00 22 Au 2004**

clock timezone <*value*>

The **clock timezone** command sets the unit's internal clock to the time zone of your choice. This setting is based on the difference in time (in hours) between Greenwich Mean Time (GMT) or Central Standard Time (CST) and the time zone for which you are setting up the unit. Use the **no** form of this command to disable this feature.

Syntax Description

<*value*>	Time zone values are specified in the *Functional Notes* section for this command.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

*Depending on the **clock timezone** chosen, one-hour daylight savings time (DST) correction may be enabled automatically. Refer to the command* *clock on page 1232* *for more information.*

Functional Notes

The following list shows sample cities and their time zone codes.

clock timezone +1-Amsterdam
clock timezone +1-Belgrade
clock timezone +1-Brussels
clock timezone +1-Sarajevo
clock timezone +1-West-Africa
clock timezone +10-Brisbane
clock timezone +10-Canberra
clock timezone +10-Guam
clock timezone +10-Hobart
clock timezone +10-Vladivostok
clock timezone +11
clock timezone +12-Auckland
clock timezone +12-Fiji
clock timezone +13
clock timezone +2-Athens
clock timezone +2-Bucharest
clock timezone +2-Cairo
clock timezone +2-Harare
clock timezone +2-Helsinki
clock timezone +2-Jerusalem
clock timezone +3-Baghdad
clock timezone +3-Kuwait
clock timezone +3-Moscow
clock timezone +3-Nairobi
clock timezone +3:30
clock timezone +4-Abu-Dhabi
clock timezone +4-Baku
clock timezone +4:30
clock timezone +5-Ekaterinburg
clock timezone +5-Islamabad
clock timezone +5:30
clock timezone +5:45
clock timezone +6-Almaty
clock timezone +6-Astana
clock timezone +6-Sri-Jay
clock timezone +6:30
clock timezone +7-Bangkok
clock timezone +7-Kranoyarsk

clock timezone +8-Bejing
clock timezone +8-Irkutsk
clock timezone +8-Kuala-Lumpur
clock timezone +8-Perth
clock timezone +8-Taipei
clock timezone +9-Osaka
clock timezone +9-Seoul
clock timezone +9-Yakutsk
clock timezone +9:30-Adelaide
clock timezone +9:30-Darwin
clock timezone -1-Azores
clock timezone -1-Cape-Verde
clock timezone -10
clock timezone -11
clock timezone -12
clock timezone -2
clock timezone -3-Brasilia
clock timezone -3-Buenos-Aires
clock timezone -3-Greenland
clock timezone -3:30
clock timezone -4-Atlantic-Time
clock timezone -4-Caracus
clock timezone -4-Santiago
clock timezone -5
clock timezone -5-Bogota
clock timezone -5-Eastern-Time
clock timezone -6-Central-America
clock timezone -6-Central-Time
clock timezone -6-Mexico-City
clock timezone -6-Saskatchewan
clock timezone -7-Arizona
clock timezone -7-Mountain-Time
clock timezone -8
clock timezone -9
clock timezone -0-Universal Coordinated Time (UTC)
clock timezone GMT-Casablanca
clock timezone GMT-Dublin

Usage Examples

The following example sets the time zone for Santiago, Chile.

>**enable**
(config)#**clock timezone -4-Santiago**

community-list *<name>*

Use the **community-list** command to create a community list for Border Gateway Protocol (BGP) route map use. Use the **no** form of this command to delete a community list.

Syntax Description

<name>	Specifies the name of the community to use in the community list attribute for BGP routes. Refer to *Community List Command Set on page 4058* for more information on the available options.

Default Values

By default, this command is disabled.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates a community list **MyList** and enters the Community List Configuration mode:

(config)**#community-list MyList**
(config-comm-list)**#**

counter-profile <*slot/index*>

Use the **counter-profile** command to create a counter-profile and enter the Counter Profile Configuration mode. Use the **no** form of this command to remove the counter profile.

Syntax Description

<*slot/index*>	Specifies the index of the counter-profile in the format <*slot/index*>. For example, **0/1**.

Default Values

By default, no counter-profiles exist.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example creates counter profile **0/1** and enters the Counter Profile Configuration mode:

(config)**#counter-profile 0/1**
(config-count-prof 0/1)**#**

quit
Hash: 4e904504dc4e5b95e08129430e2a0b97ceef0ad1394f905b42df2dfb8f751be0244a711bb0
6eddaa2f07dd640c187f14c16fa0bed28e038b28b6741a880539d6ed06a68b7e324bfdde6f3d0b17
83d94e58fd4943f5988a7a0f27f6b6b932dc041037824716075285385 8dbe7a1951245cfb14b109e
ffc430e177623720de56f4
* Do you accept this certificate? [y]**y**

crypto ca authenticate *<profile name>*

Use the **crypto ca authenticate** command to initiate certificate authority (CA) authentication procedures. Variations of this command include:

crypto ca authenticate *<profile name>*
crypto ca authenticate *<profile name> <drive> <name>*

Syntax Description

<profile name>	Specifies a CA profile using an alphanumeric string up to 32 characters.
<drive> <name>	Optional. Specifies the certificate to be authenticated is loaded from a file identified by it's location (*<drive>*), such as **nonvol**, **cflash**, etc., and the name of the file (*<name>*). This bypasses the terminal loading process.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release R11.5.0	Command was expanded to include the *<drive>* and *<name>* parameters.

Functional Notes

The type of authentication procedure is based on the **enrollment** command and its settings. Refer to *enrollment terminal on page 5213* and *enrollment url <url> on page 5214* for more information. When **enrollment** is set to **terminal**, the CA authentication process is done manually, as shown in several of the following *Usage Examples*.

Usage Examples

The following example initiates the CA authentication process for manual enrollment:

(config)**#crypto ca authenticate testCAprofile**

Enter the base 64 encoded CA certificate. End with two consecutive carriage returns or the word "quit" on a line by itself:

-----BEGIN X509 CERTIFICATE-----
MIIDEDCCAs6gAwIBAgICAXIwCwYHKoZIzjgEAwUAMFoxCzAJBgNVBAYTAkZJMSQw
IgYDVQQKExtTU0ggQ29tbXVuaWNhdGlvbnMgU2VjdXJpdHkxETAPBgNVBAsTCFdl
YiB0ZXN0MRIwEAYDVQQDEwlUZXN0IENBIDQwHhcNMDMwMTA5MTYyNTE1WhcNMDMx
MjMxMjM1OTU5WjBaMQswCQYDVQQGEwJGSTEkMCIGA1UEChMbU1NIIENvbW11bmlj
YXRpb25zIFNlY3VyaXR5MREwDwYDVQQLEwhXZWIgdGVzdDESMBAGA1UEAxMJVGVz
dCBDQSA0MIIBtzCCASsGByqGSM44BAEwggEeAoGBAPTo+NdCWh87hOSnuZ7dUL07
twjZZwY3beLHnDsERhfN8XoOZZcffulKc/lqTrYiu7M5yPJsXQ3u8dbCb6RWFU0A
T5Nd7/4cNn/hCmhbeb6xqsNZUsOcTZJxvClq8thkNo+gXg5bw0fiElgxZ/lEbFWL
UzeO8KgM4izkq0CrGtaFAhUA2+ja4RgbbgTgJk+qTXAxicG/8JMCgYBZvcPMO2/Y
Zc2sXYyrBPtv6k2ZGGYqXAUZ98/txm37JwQGafygePJ/64oeisVeDcLf2FTjveex

W5saydjSK00jXjreRZcJFEDmfRhUtWR8K8tm8mEnB3eg9n09lkWibIjihHn7n5MF
tBBAdbRHyctsr3DyofnieTt3DY78MDsNbgOBhQACgYEA6EKDS2IxrdMsogHfVvob
PkDSv2FjOsP5Tomc/tf9jvvuf6+vj9XTw+uAg1BU9/TyjGzAtnRrCvOUkTYoVxRY
vdDOi3GR2RcyNVdGrhYXWY1I5XuB5+NWij8VUQOgfXsJgbEMvPemECeYwQ4ASdhD
vw0E8NI2AEkJXsCAvYfXWzujIzAhMAsGA1UdDwQEAwIBhjASBgNVHRMBAf8ECDAG
AQH/AgEyMAsGByqGSM44BAMFAAMvADAsAhRa0ao0FbRQeWCc2oC24OZ1YZi8egIU
IZhxKAclhXksZHvOj+yIld5x0ec=
-----END X509 CERTIFICATE-----
quit
Hash: 4e904504dc4e5b95e08129430e2a0b97ceef0ad1394f905b42df2dfb8f751be0244a711bb0
6eddaa2f07dd640c187f14c16fa0bed28e038b28b6741a880539d6ed06a68b7e324bfdde6f3d0b17
83d94e58fd4943f5988a7a0f27f6b6b932dc0410378247160752853858dbe7a1951245cfb14b109e
ffc430e177623720de56f4
* Do you accept this certificate? [y]**y**

The following example initiates CA authentication for a specific file, locally stored on the AOS device, and bypasses the terminal loading process for the file:

(config)**#crypto ca authenticate MYPROFILE nonvol CA.pem**

crypto ca certificate chain <*name*>

Use the **crypto ca certificate chain** command to enter the Certificate Configuration for the specified certificate authority (CA). Refer to *Certificate Command Set on page 5221* for more information.

Syntax Description

<*name*>	Specifies a CA profile using an alphanumeric string (up to 32 characters).

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

Typically used only in the **running-config** and **startup-config** to restore certificates.

Usage Examples

The following example enters the Certificate Configuration mode for the CA profile **MyProfile**:

(config)**#crypto ca certificate chain MyProfile**

crypto ca enroll <*profile name*>

Use the **crypto ca enroll** command to begin certificate authority (CA) enrollment procedures. Use the **no** form of this command to disable this feature. Variations of this command include:

crypto ca enroll <*profile name*>
crypto ca enroll <*profile name*> **force-overwrite**
crypto ca enroll <*profile name*> <*drive*> <*name*>
crypto ca enroll <*profile name*> <*drive*> <*name*> **force-overwrite**

Syntax Description

<*profile name*>	Specifies a CA profile using an alphanumeric string (up to 32 characters).
<*drive*> <*name*>	Optional. Specifies the certificate to be enrolled is loaded from a file identified by it's location (<*drive*>), such as **nonvol**, **cflash**, etc., and the name of the file (<*name*>). This bypasses the terminal loading process.
force-overwrite	Optional. Instructs the AOS device to overwrite any existing file with the same name. If the <*drive*> and <*name*> parameters are not specified, the enrollment dialog prompts you to indicate if the certificate request should be written to a file, and if yes, the drive and filename to use. If the certificate request is not saved to file, the keys remain and the request is discarded.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release R11.5.0	Command was expanded to include the <*drive*>, <*name*>, and **force-overwrite** parameters.

Functional Notes

The type of enrollment procedure is based on the **enrollment** command and its settings. Refer to *enrollment terminal on page 5213* and *enrollment url <url> on page 5214* for more information. This command initiates a dialog that is used to fill in the parameters that make up an enrollment request to be forwarded to a certificate authority. Note that some of the parameters (such as IP address) may be filled in using the values supplied in the **crypto ca profile** (in which case, the enrollment dialog will not prompt for those parameters). Once all required parameters are defined using the dialog, this command assembles them into an enrollment request to be sent to a certificate authority (including the generation of public and private keys). Refer to *crypto ca profile <name> on page 1246* for more information.

If **enrollment** is set to **terminal**, you may view the request on the terminal screen.

If **enrollment** is set to **url**, the request is sent automatically to the certificate authority using the uniform resource locator (URL) specified by the **enrollment url** command.

Usage Examples

The following example shows a typical enrollment dialog:

(config)**#crypto ca enroll MyProfile**
**** Press CTRL+C to exit enrollment request dialog. ****
* Enter signature algorithm (RSA or DSS) [rsa]:**rsa**
* Enter the modulus length to use [512]:**1024**
* Enter the subject name as an X.500 (LDAP) DN:**CN=Router,C=US,L=Huntsville,S=AL**
--The subject name in the certificate will be CN=CN=Router,C=US,L=Huntsville,S=AL.
* Include an IP address in the subject name [n]:**y**
* Enter IP address or name of interface to use:**10.200.1.45**
* Include fully qualified domain name [n]:**y**
* Enter the fully qualified domain name to use:**FullyQualifiedDomainName**
* Include an email address [n]:**y**
* Enter the email address to use:**myEmail@adtran.commyemail@email.com**
Generating request (including keys).

The following example creates a CA certificate and begins the enrollment process using a locally stored file:

(config)**#crypto ca enroll MYPROFILE novol SELF.csr force-overwrite**

crypto ca import <*profile name*> certificate

Use the **crypto ca import certificate** command to import a certificate manually via the console terminal. Variations of this command include:

crypto ca import <*profile name*> **certificate**
crypto ca import <*profile name*> **certificate** <*drive*> <*name*>

Syntax Description

<*profile name*>	Specifies a certificate authority (CA) profile using an alphanumeric string (up to 32 characters).
<*drive*> <*name*>	Optional. Specifies the certificate to be imported is loaded from a file identified by it's location (<*drive*>), such as **nonvol**, **cflash**, etc., and the name of the file (<*name*>). This bypasses the terminal loading process.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release R11.5.0	Command was expanded to include the <*drive*> and <*name*> parameters.

Functional Notes

Puts command line interface (CLI) in mode where the certificate can be entered manually. Enter **quit** and a carriage return (or simply enter two consecutive carriage returns) to exit this mode. Abort this mode by pressing **Ctrl-C**. This command only applies if the **enrollment** command is set to **terminal**. Refer to *enrollment terminal on page 5213*.

Usage Examples

The following example imports a certificate via the console terminal:

(config)**#crypto ca import MyProfile certificate**
Enter the PM-encoded certificate. End with two consecutive
carriage returns or the word "quit" on a line by itself:
-----BEGIN CERTIFICATE-----
MIIDWTCCAwOgAwIBAgIKFLCsOgAAAAAAtjANBgkqhkiG9w0BAQUFADBjMQswCQYD
VQQGEwJVUzEQMA4GA1UECBMHQUxBQkFNQTETMBEGA1UEBxMKSHVudHN2aWxsZTEa
MBgGA1UEChMRQWR0cmFuVGVjaFN1cHBvcnQxETAPBgNVBAMTCHRzcm91dGVyMB4X
DTAzMDYyNTE0MTM1NVoXDTAzMTIwNjE0NDkxM1owJDEPMA0GA1UEChMGYWR0cmFu
MREwDwYDVQQDEwhNeVJvdXRlcjBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQClUKqs
fbTalej5m9gk2DMsbC9df3TilBz+7nRx3ZzGw75AQsqEMYeBY5aWi62W59jmxGSE
WX+E8EwBVbZ6JKk5AgMBAAGjggHWMIIB0jAXBgNVHREEEDAOhwQKCgoKggZNeUZx
ZG4wHQYDVR0OBBYEFJAvBRIjx1PROnkZ4v0D89yB1eErMIGcBgNVHSMEgZQwgZGA
FHGwIRAr11495MgrLNPiLzjvrb4JoWekZTBjMQswCQYDVQQGEwJVUzEQMA4GA1UE
CBMHQUxBQkFNQTETMBEGA1UEBxMKSHVudHN2aWxsZTEaMBgGA1UEChMRQWR0cmFu

VGVjaFN1cHBvcnQxETAPBgNVBAMTCHRzcm91dGVyghAZql7OwISgsUhfaSeGh0Ot
MGkGA1UdHwRiMGAwLaAroCmGJ2h0dHA6Ly90c3JvdXRlci9DZXJ0RW5yb2xsL3Rz
cm91dGVyLmNybDAvoC2gK4YpZmlsZTovL1xcdHNyb3V0ZXJcQ2VydEVucm9sbFx0
c3JvdXRlci5jcmwwgY0GCCsGAQUFBwEBBIGAMH4wPAYIKwYBBQUHMAKGMGh0dHA6
Ly90c3JvdXRlci9DZXJ0RW5yb2xsL3Rzcm91dGVyX3Rzcm91dGVyLmNydDA+Bggr
BgEFBQcwAoYyZmlsZTovL1xcdHNyb3V0ZXJcQ2VydEVucm9sbFx0c3JvdXRlcl90
-----END CERTIFICATE-----
Success!

The following example specifies that locally stored **SELF.pem** is imported for CA profile **MYPROFILE**:

(config)**#crypto ca import MYPROFILE certificate nonvol SELF.pem**

crypto ca import <*profile name*> crl

Use the **crypto ca import crl** command to import a certificate revocation list (CRL) manually via the console terminal. Variations of this command include:

crypto ca import <*profile name*> **crl**
crypto ca import <*profile name*> **crl** <*drive*> <*name*>

Syntax Description

<*profile name*>	Specifies a certificate authority (CA) profile using an alphanumeric string (up to 32 characters).
<*drive*> <*name*>	Optional. Specifies the certificate to be imported is loaded from a file identified by it's location (<*drive*>), such as **nonvol**, **cflash**, etc., and the name of the file (<*name*>). This bypasses the terminal loading process.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release R11.5.0	Command was expanded to include the <*drive*> and <*name*> parameters.

Functional Notes

Puts command line interface (CLI) in a mode where the CRL can be entered manually. Enter **quit** and a carriage return (or simply enter two consecutive carriage returns) to exit this mode. This command only applies if the **enrollment** command is set to **terminal**. Refer to *enrollment terminal on page 5213*.

Usage Examples

The following example allows you to manually paste in the CA's CRL:

(config)**#crypto ca import MYPROFILE crl**

The following example allows you to paste a locally stored file into the CA's CRL:

(config)**#crypto ca import MYPROFILE crl nonvol SELF.pem**

crypto ca profile *<name>*

Use the **crypto ca profile** command to define a certificate authority (CA) and to enter the CA Profile Configuration. Use the **no** form of this command to disable this feature. Refer to *CA Profile Command Set on page 5209* for more information.

Syntax Description

<name>	Creates a CA profile using an alphanumeric string (up to 32 characters).

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

Use this to specify the type of enrollment, as well as enrollment request parameters. Refer to the *Functional Notes* of the command *crypto ca enroll <profile name> on page 1241* for more information.

Usage Examples

The following example creates the CA profile called **MyProfile** and enters the CA Profile Configuration for that certificate authority:

```
(config)#crypto ca profile MyProfile
Configuring New CA Profile MyProfile.
(ca-profile)#
```


crypto ike

Use the **crypto ike** command to define the system-level local ID for Internet key exchange (IKE) negotiations and to enter the IKE Client or IKE Policy command sets. Use the **no** form of this command to disable these features. Variations of this command include the following:

crypto ike client configuration pool <*name*>
crypto ike local-id address
crypto ike policy <*value*>

Syntax Description

client configuration pool <*name*>	Creates a local pool, assigns it the name of your choice and enters the IKE Client command set. Clients that connect via an IKE policy that specifies this pool name will be assigned values from this pool. Refer to the section *IKE Policy Command Set on page 5280* for more information.
local-id address	Sets the local ID during IKE negotiation to be the IP address of the interface from which the traffic exits. This setting can be overridden on a per-policy basis using the **local-id** command. Refer to *local-id on page 5287* for more information.
policy <*value*>	Creates an IKE policy, assigns the sequence number value of your choice, and enters the IKE Policy command set. Refer to section *IKE Policy Command Set on page 5280* for more information.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example creates an IKE policy with a policy priority setting of 1 and enters the IKE Policy for that policy:

(config)**#crypto ike policy 1**

Technology Review

The following example configures an AOS product for virtual private network (VPN) using IKE aggressive mode with preshared keys (PSKs). The AOS product can be set to initiate IKE negotiation in main mode or aggressive mode. The product can be set to respond to IKE negotiation in main mode, aggressive mode, or any mode. In this example, the device is configured to initiate in aggressive mode and to respond to any mode.

This example assumes that the AOS product has been configured with a wide area network (WAN) IP address of **63.97.45.57** on interface **ppp 1** and a local area network (LAN) IP address of **10.10.10.254** on interface **ethernet 0/1**. The peer private IP Subnet is **10.10.20.0**.

Step 1:
Enter the Global Configuration mode (i.e., config terminal mode).

>**enable**
#configure terminal

Step 2:
Enable VPN support using the **ip crypto** command. This command allows crypto maps to be applied to interfaces, and enables the IKE server to listen for IKE negotiation sessions on User Datagram Protocol (UDP) port 500.

(config)**#ip crypto**

Step 3:
Set the local ID. During IKE negotiation, local IDs are exchanged between the local device and the peer device. In AOS, the default setting for all local IDs are configured by the **crypto ike local-id** command. The default setting is for all local IDs to be the IPv4 address of the interface over which the IKE negotiation is occurring. In the future, a unique system-wide host name or fully qualified domain name (FQDN) could be used for all IKE negotiation.

(config)**#crypto ike local-id address**

Step 4:
Create IKE policy. In order to use IKE negotiation, an IKE policy must be created. Within the system, a list of IKE policies is maintained. Each IKE policy is given a priority number in the system. That priority number defines the position of that IKE policy within the system list. When IKE negotiation is needed, the system searches through the list, starting with the policy with priority of 1, looking for a match to the peer IP address.

An individual IKE policy can override the system local ID setting by having the **local-id** command specified in the IKE policy definition. This command in the IKE policy is used to specify the type of local ID and the local ID data. The type can be of IPv4 address, FQDN, or user-specified FQDN.

An IKE policy may specify one or more peer IP addresses that will be allowed to connect to this system. To specify multiple unique peer IP addresses, the **peer A.B.C.D** command is used multiple times within a single IKE policy. To specify that all possible peers can use a default IKE policy, the **peer any** command is given instead of the **peer A.B.C.D** command inside of the IKE policy. The policy with the **peer any** command specified will match to any peer IP address (and, therefore, should be given the highest numerical priority number). This will make the policy the last one to be compared against during IKE negotiation.

(config)**#crypto ike policy 10**
(config-ike)**#no local-id**
(config-ike)**#peer 63.105.15.129**
(config-ike)**#initiate aggressive**
(config-ike)**#respond anymode**
(config-ike)**#attribute 10**
(config-ike-attribute)**#encryption 3des**
(config-ike-attribute)**#hash sha**
(config-ike-attribute)**#authentication pre-share**
(config-ike-attribute)**#group 1**
(config-ike-attribute)**#lifetime 86400**

Step 5:
Define the remote ID settings. The **crypto ike remote-id** command is used to define the remote ID for a peer connecting to the system, specify the preshared key associated with the specific remote ID, and (optionally) determine that the peer matching this remote ID should not use mode config (by using the **no-mode-config** keyword). Refer to *crypto ike remote-id on page 1251* for more information.

(config)**#crypto ike remote-id address 63.105.15.129 preshared-key mysecret123**

Step 6:
Define the transform-set. A transform set defines the encryption and/or authentication algorithms to be used to secure the data transmitted over the VPN tunnel. Multiple transform sets may be defined in a system. Once a transform set is defined, many different crypto maps within the system can reference it. In this example, a transform set named **highly_secure** has been created. This transform set defines encapsulating security payload (ESP) with authentication implemented using 3DES encryption and SHA1 authentication.

(config)**#crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac**
(cfg-crypto-trans)**#mode tunnel**

Step 7:
Define an IP access list. An extended access control list (ACL) is used to specify which traffic needs to be sent securely over the VPN tunnel. The entries in the list are defined with respect to the local system. The source IP address will be the source of the traffic to be encrypted. The destination IP address will be the receiver of the data on the other side of the VPN tunnel.

(config)**#ip access-list extended corporate_traffic**
(config-ext-nacl)**#permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255 log deny ip any any**

Step 8:
Create crypto map. A crypto map is used to define a set of encryption schemes to be used for a given interface. A crypto map entry has a unique index within the crypto map set. The crypto map entry will specify whether IKE is used to generate encryption keys or if manually specified keys will be used. The crypto map entry will also specify who will be terminating the VPN tunnel, as well as which transform set or sets will be used to encrypt and/or authenticate the traffic on that VPN tunnel. It also specifies the lifetime of all created IPSec security associations (SAs).

(config)**#crypto map corporate_vpn 1 ipsec-ike**
(config-crypto-map)**#match address corporate_traffic**
(config-crypto-map)**#set peer 63.105.15.129**
(config-crypto-map)**#set transform-set highly_secure**
(config-crypto-map)**#set security-association lifetime kilobytes 8000**
(config-crypto-map)**#set security-association lifetime seconds 28800**
(config-crypto-map)**#no set pfs**

Step 9:
Configure a public interface. This process includes configuring the IP address for the interface and applying the appropriate crypto map to the interface. Crypto maps are applied to the interface on which encrypted traffic will be transmitted.

(config)**#interface ppp 1**
(config-ppp 1)**#ip address 63.97.45.57 255.255.255.248**
(config-ppp 1)**#crypto map corporate_vpn**
(config-ppp 1)**#no shutdown**

Step 10:
Configure a private interface. This process allows all traffic destined for the VPN tunnel to be routed to the appropriate gateway.

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip address 10.10.10.254 255.255.255.0**
(config-eth 0/1)**#no shutdown**
(config-eth 0/1)**#exit**

crypto ike remote-id

Use the **crypto ike remote-id** command to specify the remote ID and to associate a preshared key with the remote ID. Use the **no** form of this command to disable these features. Variations of this command include the following:

crypto ike remote-id address <*ip address*>
crypto ike remote-id address <*ip address*> <*option*>
crypto ike remote-id any
crypto ike remote-id any <*option*>
crytpo ike remote-id asn1-dn <*name*>
crypto ike remote-id asn1-dn <*name*> <*option*>
crypto ike remote-id fqdn <*name*>
crypto ike remote-id fqdn <*name*> <*option*>
crypto ike remote-id user-fqdn <*name*>
crypto ike remote-id user-fqdn <*name*> <*option*>

*The AOS virtual private network (VPN) feature must be enabled (using the **ip crypto** command) for the VPN tunnel to be activated.*

Syntax Description

address <*ip address*>	Specifies a valid remote IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
any	Allows any remote ID (type and value).
asn1-dn <*name*>	Specifies an abstract syntax notation distinguished name as the remote ID (enter this value in (Lightweight Directory Access Protocol (LDAP) format).
fqdn <*name*>	Specifies a fully qualified domain name (FQDN) (e.g., **adtran.com**) as the remote ID.
user-fqdn <*name*>	Specifies a user FQDN or email address (e.g., **user1@adtran.com**) as the remote ID.
<*option*>	Specifies an optional parameter corresponding to this remote ID. Optional parameters include the following list:
<*wildcard mask*>	Optional. Specifies the wildcard mask that corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
crypto map <*name*> <*number*>	Optional. Specifies the crypto map name and sequence number this remote ID corresponds to.
ike policy <*value*>	Optional. Specifies the Internet key exchange (IKE) policy sequence number value this remote ID corresponds to.
preshared-key <*key*>	Optional. Associates a preshared key with this remote ID.

no-mode-config	Optional. Specifies that the peer matching this remote ID should not use mode config.
no-xauth	Optional. Specifies that the peer matching this remote ID should not use Xauth.
nat-t [v1 l v2] [allow l force l disable]	Optional. Denotes whether peers matching this remote ID should allow, disable, or force network address translation (NAT) traversal versions 1 or 2.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the **any**, **asn1-dn**, and **no-xauth** subcommands.
Release 7.1	Command was expanded to include the NAT traversal commands.

Functional Notes

The **fqdn** and **user-fqdn** <*fqdn*> line can include wildcard characters. The wildcard characters are "*****" for a 0 or more character match and "?" for a single character match. Currently, the "?" cannot be set up using the command line interface (CLI), but it can be transferred to the unit via the startup-config.

Example for **user-fqdn**:

john*@domain.com

will match:

johndoe@domain.com
johnjohn@adtran.comjohnjohn@myemail.com
john@adtran.comjohn@myemail.com

Example for **fqdn**:

***.domain.com**

will match:

www.domain.com
ftp.domain.com
one.www.domain.com

The **address** remote ID can be in the form of a single host address or in the form of an IP address wildcard.

Example for **address** type:

crypto ike remote id address 10.10.10.0 0.0.0.255

will match:

10.10.10.1
10.10.10.2
and all IP addresses in the form of 10.10.10.X (where X is 0 to 255)

The **asn1-dn** <*name*> line can include wildcard characters. The wildcard characters are "*" for a 0 or more character match and "?" for a single character match. Currently, the "?" cannot be set up using the CLI, but it can be transferred to the unit via the startup-config.

Example for typical **asn1-dn** format with no wildcards:

crypto ike remote-id asn1-dn "CN=MyRouter, C=US, S=ALCA, L=Huntsville, O=Adtran, OU=TechSupport"
(matches only remote ID strings with all fields exactly the same)

Example for typical **asn1-dn** format with wildcards used to match a string within a field:

crypto ike remote-id asn1-dn "CN=*, C=*, S=*, L=*, O=*, OU=*"
(matches any asn1-dn remote ID string from a peer)

Example for typical **asn1-dn** format with wildcards used to match a portion of the remote ID:

crypto ike remote-id asn1-dn "CN=*, C=US, S=ALCA, L=Huntsville, O=Adtran, OU=*"
(matches any remote ID string with the same values for the C, S, L, and O fields, and any values in the CN and OU fields)

Example for typical **asn1-dn** format with wildcards used to match a portion of a field:

crypto ike remote-id asn1-dn "CN=My*, C=US, S=ALCA, L=Huntsville, O=Adtran, OU=TechSupport"
(matches remote ID strings with all fields exactly the same, but with any CN field beginning with "My")

Usage Examples

The following example assigns a remote ID of 63.97.45.57 and associates the preshared key **mysecret** with the remote ID:

(config)**#crypto ike remote-id address 63.97.45.57 preshared-key mysecret**

data-call

Use the **data-call** command to set the preauthentication defaults for inbound demand routing calls. Use the **no** form of this command to return to the default setting. Variations of this command include:

data-call authentication protocol chap
data-call authentication protocol pap
data-call mtu <*number*>
data-call multilink
data-call sent authentication protocol chap
data-call sent authentication protocol pap

Syntax Description

authentication protocol	Sets the authentication protocol expected for inbound calls. For more detailed information on Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP), refer to the *Technology Review* section of the command *ppp authentication on page 3192*.
chap	Configures CHAP authentication.
pap	Configures PAP authentication.
mtu <*number*>	Sets the maximum size for the transmit unit. Valid range is **64** to **1520**. Refer to the command *peer default ip address <ipv4 address> on page 3190* for more detailed syntax descriptions.
multilink	Enables the negotiation of multilink maximum receive unit (MRU) size for inbound calls.
sent authentication protocol	Sets the authentication protocol sent for inbound calls. For more detailed information on CHAP and PAP, refer to the *Technology Review* section of the command *ppp authentication on page 3192*.

Default Values

By default, the authentication protocol is not configured, multilink is disabled, and the maximum transmission unit (MTU) size is 1500.

Command History

Release 11.1	Command was introduced.

Functional Notes

There are certain Point-to-Point Protocol (PPP) parameters that must be known before PPP can negotiate an inbound call when using demand routing. To ensure PPP convergence, it is recommended (in most cases) that demand routing interfaces use the same settings as those specified in the **data-call** commands. The **data-call mtu** <*number*> command sets the MTU and controls the negotiated MRU size during incoming calls for Link Control Protocol (LCP) negotiation. If the PPP parameters do not match the authenticated user, the link is renegotiated.

Usage Examples

The following example sets the authentication protocol expected for incoming calls to CHAP. The router will then authenticate the peer using CHAP:

(config)**#data-call authentication protocol chap**

The following example specifies an MTU of 1200 on the demand routing interface:

(config)**#data-call mtu 1200**

data-plane cpu mode

Use the **data-plane cpu mode** command to specify the mode in which virtual AOS (vAOS) operates on the central processing unit (CPU) of the host server. Use the **no** form of this command to return to the default setting. Variations of this command include:

data-plane cpu mode shared
data-plane cpu mode dedicated

Syntax Description

shared	Specifies that vAOS shares the data forwarding plane CPU with other processes.
dedicated	Specifies that vAOS does not share the data forwarding plane CPU with other processes.

Default Values

By default, the vAOS CPU mode is set to **shared**.

Command History

Release R12.1.0	Command was introduced.

Functional Notes

The **shared** mode is useful when other processes on the CPU must take priority over a vAOS instance, or when multiple vAOS instances are stacked on a set of CPUs. Setting the vAOS mode to **shared** may result in lower throughput. The **dedicated** mode is useful when the data forwarding plane CPU does not need to be shared or when maximizing throughput.

Usage Examples

The following example specifies that vAOS does not share the data forwarding plane CPU with any other processes:

(config)**#data-plane cpu mode dedicated**

desktop-auditing dhcp

Use the **desktop-auditing dhcp** command to enable desktop auditing. Using the **no** form of this command disables desktop auditing.

Syntax Description

No subcommands.

Default Values

By default, desktop auditing is disabled.

Command History

Release 17.8	Command was introduced.

Functional Notes

Desktop auditing is an AOS feature that collects network access protection (NAP) information through NAP messages sent in Dynamic Host Configuration Protocol (DHCP) messages between clients connected to the network and the network server.

Desktop auditing is configured by enabling the feature (using the **desktop-auditing dhcp** command) and by configuring filters to limit the output of the collected NAP information. Information is limited by specifying local desktop auditing policies. The configuration of these policies is outlined in *Desktop Auditing Local Policy Command Set on page 4395*. For more information about desktop auditing, refer to the *Configuring Desktop Auditing in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables the desktop auditing feature:

(config)**#desktop-auditing dhcp**

desktop-auditing local-policy

Use the **desktop-auditing local-policy** command to create a local policy for determining when connected network clients are violators of that policy. This command both creates the policy and enters the local policy configuration mode. Use the **no** form of this command to remove the local policy.

Command Syntax

No subcommands.

Default Values

By default, no local policies are configured and all network access protection (NAP) information for all clients is monitored.

Command History

Release 17.8	Command was introduced.

Functional Notes

Desktop auditing is an AOS feature that collects NAP information through NAP messages sent in Dynamic Host Configuration Protocol (DHCP) messages between clients connected to the network and the network server.

Desktop auditing is configured by enabling the feature (using the command *desktop-auditing dhcp on page 1257*) and by configuring filters to limit the output of the collected NAP information. Information is limited by specifying local desktop auditing policies. The local policy determines when a network access protection (NAP) client may be a violator by collecting NAP information for the connected clients and comparing them to the configured policies. You can choose to monitor the client's firewall state, antivirus state, antispyware status, auto-update status, and security update status. Selecting these policies filters the collected client information.

The configuration of these policies is outlined in *Desktop Auditing Local Policy Command Set on page 4395*. For more information about desktop auditing, refer to the *Configuring Desktop Auditing in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a desktop auditing local policy and enters the policy's configuration mode:

```
(config)#desktop-auditing local-policy
(desktop-audit-policy)#
```

desktop-auditing timeout <*days*>

Use the **desktop-auditing timeout** command to specify the amount of time that the AOS unit keeps network access protection (NAP) information collected through desktop auditing. Use the **no** form of this command to return to the default timeout period.

Syntax Description

<*days*>	Specifies the amount of time (in days) that desktop auditing stores collected NAP information. Range is **0** to **49710**.

Default Values

By default, desktop auditing is set to timeout in **0** days, meaning the collected NAP information is stored indefinitely.

Command History

Release 17.8	Command was introduced.

Functional Notes

Desktop auditing is an AOS feature that collects NAP information through NAP messages sent in Dynamic Host Configuration Protocol (DHCP) messages between clients connected to the network and the network server.

Desktop auditing is configured by enabling the feature (using the **desktop-auditing dhcp** command) and by configuring filters to limit the output of the collected NAP information. Information is limited by specifying local desktop auditing policies. The configuration of these policies is outlined in *Desktop Auditing Local Policy Command Set on page 4395*. For more information about desktop auditing, refer to the *Configuring Desktop Auditing in AOS* configuration guide available online at https://supportcommunity.adtran.com.

There is a storage limit of **2000** NAP entries on the AOS unit. When this limit is reached, new entries overwrite the old entries.

Usage Examples

The following example specifies that NAP information collected by desktop auditing will expire in **7** days:

(config)**#desktop-auditing timeout 7**

domain-list *<domain>*

Use the **domain-list** command to add an entry to the Domain Name Server (DNS) domain list. DNS appends the listed domains to a host name when attempting to resolve it. Use the **no** form of this command to remove the domain list entry. Variations of this command include:

domain-list <*domain*>
domain-list vrf <*name*> <*domain*>

Syntax Description

<*domain*>	Specifies the domain on which to create the domain list entry.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to create the domain list entry. If no VRF is specified, the entry is created on the default VRF.

Default Values

By default, no domain list entries exist.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example creates a domain list entry for **DOMAIN1** on the default VRF instance:

(config)**#domain-list DOMAIN1**

domain-lookup

Use the **domain-lookup** command to enable and configure the IPv4 or IPv6 domain naming system (DNS), allowing DNS-based host translation (name-to-address). Use the **no** form of this command to disable DNS. Variations of this command include:

domain-lookup database local
domain-lookup database local ttl <*value*>
domain-lookup flush on-server-change
domain-lookup snmp trap first-failure
domain-lookup source-interface <*interface*>
domain-lookup vrf <*vrf name*> **source-interface** <*interface*>

Syntax Description

database local	Specifies that a local file of the DNS table is stored on the AOS device. This file is used to save the DNS table across a unit reboot.
ttl <*value*>	Optional. Specifies the time to live (TTL) value of the DNS file stored locally on the system. Valid range is **60** to **86400** seconds.
flush on-server-change	Specifies that the DNS cache is cleared when the set of configured and learned DNS servers has changed.
snmp trap first-failure	Specifies that Simple Network Management Protocol (SNMP) traps are used to send notifications when the first attempt at DNS resolution fails. In order to use SNMP traps for DNS resolution failure, you must also enable SNMP application traps using the command *snmp-server enable traps on page 1792*.
source-interface <*interface*>	Specifies an interface whose IP address will be used as the source IP address in a DNS request. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **domain-lookup source-interface ?** for a complete list of valid interfaces.
vrf <*vrf name*>	Optional. Specifies a nondefault VRF instance on which to change the source interface address for DNS requests. If no VRF instance is specified, the name server is added on the default unnamed VRF instance.

Default Values

By default, DNS is enabled; however, the **local**, **snmp trap**, and **source-interface** features of the domain lookup configuration are disabled by default. When the **local** DNS feature is enabled, the TTL value is **3600** seconds (one hour) by default.

Command History

Release 3.1	Command was introduced.

Release 18.3	Command syntax was changed to remove the **ip** keyword for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.
Release R10.3.0	Command was expanded to include the **local**, **snmp trap**, **source-interface**, and **vrf** parameters.
Release R13.2.0	Command was expanded to include the **flush on-server-change** parameter.

Functional Notes

Use the **domain-lookup** command to enable the DNS client in the router. This will allow the user to input Web addresses instead of IPv4 or IPv6 addresses for applications such as ping, Telnet, and traceroute.

Usage Examples

The following example enables DNS:

(config)**#domain-lookup**

The following example enables DNS and specifies that a local copy of the DNS table is saved on the AOS unit:

(config)**#domain-lookup local**

The following example enables DNS and DNS SNMP reporting:

(config)**#snmp-server enable traps application**
(config)**#domain-lookup snmp trap first-failure**

The following example enables DNS and specifies that the IP address of the **VLAN 1** interface on the VRF instance **RED** is used for DNS requests:

(config)#d**omain-lookup vrf RED source-interface vlan 1**

domain-name <*domain name*>

Use the **domain-name** command to define a default IPv4 or IPv6 domain name to be used by AOS to resolve host names. Use the **no** form of this command to disable this function. Variations of this command include:

domain-name <*domain name*>
domain-name vrf <*name*> <*domain name*>

Syntax Description

<*domain name*>	Specifies the default IPv4 or IPv6 domain name used to resolve unqualified host names. Do not include the initial period that separates the unresolved name from the default domain name.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance for the domain name.

Default Values

By default, this command is disabled.

Command History

Release 3.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command syntax was changed to remove the **ip** keyword for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Functional Notes

Use the **domain-name** command to set a default name that will be used to complete any IPv4 or IPv6 host name that is invalid (i.e., any name that is not recognized by the name server). When this command is enabled, any IPv4 or IPv6 host name that is not initially recognized will have the **domain-name** appended to it and the request will be re-sent.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Each VRF instance has its own domain name. Specifying a VRF name in the command applies the domain name to the named VRF. Issuing the command without specifying a VRF applies the command to the default unnamed VRF.

Usage Examples

The following example defines **adtran** as the default domain name:

(config)**#domain-name adtran**

The following example defines **adtran** as the default domain name for the VRF **RED**:

(config)**#domain-name vrf RED adtran**

domain-proxy

Use the **domain-proxy** command to enable domain naming system (DNS) proxy for the default virtual routing and forwarding (VRF) or for a specified VRF instance. This enables the router to act as a proxy for other units on the network. Use the **no** form of this command to disable this feature. Variations of this command include:

domain-proxy
domain-proxy failover
domain-proxy source-interface <*interface*>
domain-proxy vrf <*name*>
domain-proxy vrf <*name*> **failover**
domain-proxy vrf <*name*> **source-interface** <*interface*>

Syntax Description

failover	Enables DNS failover mode on the default domain proxy.
source-interface <*interface*>	Optional. Specifies the source interface for DNS packets. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Valid interfaces are those that can have an IP address. Type **source ?** for a complete list of valid interfaces.
vrf <*name*>	Optional. Specifies a nondefault VRF on which to enable DNS proxy.

Default Values

By default, this command is disabled.

Command History

Release 3.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 17.9	Command was expanded to include the **source-interface** parameter.
Release 18.2	Command was expanded to include the **failover** parameter.
Release 18.3	Command syntax was changed to remove the **ip** keyword for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.
Release R10.3.0	Command was expanded to include the **vrf** parameter for **source-interface** configurations.

Functional Notes

When this command is enabled, incoming DNS requests will be handled by the router. It will first search its host table for the query, and if it is not found there, the request will be forwarded to the servers configured with the command *name-server on page 1622*.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

DNS failover allows the AOS unit to respond to a DNS request if the unit cannot reach the configured DNS server and the entry exists in the unit's DNS table as a preserved value. DNS failover is typically used with the Voice of Internet Protocol (VoIP) name-server caching feature.

Usage Examples

The following example enables DNS proxy on the default VRF (router):

(config)**#domain-proxy**

dos-protection

Use the **dos-protection** command to enable and configure the denial of service (DoS) protection feature. Use the **no** form of this command to disable the DoS protection feature. Variations of this command include:

dos-protection all
dos-protection except <*id*>
dos-protection max-icmpv4-payload <*bytes*>
dos-protection max-icmpv6-payload <*bytes*>
dos-protection min-tcp-header <*bytes*>

Syntax Description

all	Enables protection from all DoS attacks available in the feature.
except <*ids*>	Enables protection from all available DoS attacks except those with the listed threat *ids*.
max-icmpv4-payload <*bytes*>	Sets the maximum ICMP payload size in bytes for IPv4 packets. Range is **0** to **16** KB. Default is **512** bytes.
max-icmpv6-payload <*bytes*>	Sets the maximum ICMP payload size in bytes for IPv6 packets. Range is **0** to **16** KB. Default is **512** bytes.
min-tcp-header <*bytes*>	Sets the minimum TCP header size in bytes. Range is **0** to **255** bytes. Default is **20** bytes.

Default Values

By default, DoS protection in AOS is disabled.

Command History

Release 17.7	Command was introduced.

Functional Notes

The **show dos-id** command is used to obtain the DoS threat IDs necessary to create exceptions using the **dos-protection except** <*id*> version of this command.

Usage Examples

The following example configures the DoS protection feature to protect against all available threats except threat ID **40**:

(config)**#dos-protection except 40**

dot11ap access-point-control

Use the **dot11ap access-point-control** command to globally enable the access point controller logic on the platform. Use the **no** form of this command to disable the access controller (AC) logic on the platform.

Syntax Description

No subcommands.

Default Values

By default, the AC logic is disabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example enables the AC logic:

(config)**#dot11ap access-point-control**

dynamic-counter <*slot/index*>

Use the **dynamic-counter** command to create a dynamic counter and enter the Dynamic Counter Configuration mode. Use the **no** form of this command to remove the dynamic counter.

Syntax Description

<*slot/index*>	Specifies the slot and port of the dynamic counter in the format <*slot/index*>. For example, **0/1**.

Default Values

By default, no dynamic counters exist.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example creates dynamic counter **0/1** and enters the Dynamic Counter Configuration mode:

```
(config)#dynamic-counter 0/1
(config-dyn-count 0/1)#
```

enable password *<password>*

Use the **enable password** command to define a password (with optional encryption and privilege level) for accessing the Enable mode. Use the **no enable password** command to remove a configured password. Variations of this command include:

enable password level *<level> <password>*
enable password md5 *<password>*
enable password md5 level *<level> <password>*
enable password *<password>*

To prevent unauthorized users from accessing the configuration functions of your device, immediately define an Enable-level password.

Syntax Description

level *<level>*	Optional. Specifies the privilege level for this enable password. Valid range is **1** through **7**.
md5	Optional. Specifies message digest 5 (MD5) as the encryption protocol to use when displaying the Enable password during show commands. If the **md5** keyword is not used, encryption is not used when displaying the Enable password during show commands.
<password>	Specifies the Enable password using a string (up to 30 characters in length).

Default Values

By default, there is no password configured for the Enable mode. By default, when an enable password is configured without specifying a privilege level, the privilege level assigned is 7.

Command History

Release 1.1	Command was introduced.
Release R10.11.0	Command was expanded to include the **level** parameter.

Usage Examples

The following example configures the enable password as **Adtran** with **md5** encryption, and specifies privilege level **4**:

(config)**#enable password md5 level 4 Adtran**
!

To provide extra security, AOS can encrypt the Enable password when displaying the current configuration. For example, the following is a **show configuration** printout (password portion) with an unencrypted Enable password (Adtran):

```
!
enable password Adtran
!
```

Alternately, the following is a **show configuration** printout (password portion) with an Enable password of Adtran using MD5 encryption:

```
!
enable password md5 encrypted 5aa5fbae7d01a90e79fb57705ce74676
!
```

ethernet ce-vlan-tpid *<value>*

Use the **ethernet ce-vlan-tpid** command to specify that tag protocol identifiers (TPIDs) other than 0x8100 are accepted on the user network interface (UNI) that is matching on customer edge (CE) virtual local area network (VLAN) ID or priority. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the hexadecimal value of the EtherType to accept, for example, **0x88a8**.

Default Values

By default, no special global handling of TPIDs is configured, and Ethernet virtual connection (EVC) maps accept and process packets with a CE VLAN TIPID of 0x8100.

Command History

Release R11.6.0	Command was introduced.

Functional Note

All EVC maps default to the globally-specified EtherType for CE VLAN ID matching. In addition, all EVC maps default to using the specified EtherType for adding CE VLAN IDs to traffic flowing in the Metro Ethernet Network (MEN) to UNI direction when the CE VLAN ID is not preserved as well as using the specified EtherType for adding c-tags to traffic flowing in the UNI to MEN direction. For more information, refer to the *Carrier Ethernet Services in AOS* configuration guide available online at https://supportcommunity.adtran.com.

You can override the global setting to return to the default value of 0x8100 on a per-map basis using the **no ce-vlan-tpid** command from the EVC map's configuration mode.

Usage Examples

The following example globally configures the accepted CE VLAN EtherType as **0x88a8**:

(config)**#ethernet ce-vlan-tpid 0x88a8**

ethernet cfm

Use the **ethernet cfm** command to enable Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) on the AOS device. Use the **no** form of this command to disable Ethernet OAM CFM.

Syntax Description

No subcommands.

Default Values

By default, Ethernet OAM CFM is disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

For more information regarding specific Ethernet OAM CFM configuration commands, refer to the *Ethernet OAM CFM Command Set on page 4405*.

Usage Examples

The following example enables Ethernet OAM CFM on an AOS device:

(config)**#ethernet cfm**

ethernet cfm domain

Use the **ethernet cfm domain** command to enable and create an Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance domain (MD). Use the **no** form of this command to remove the MD. Variations of this command include:

ethernet cfm domain <*name*> **level** <*level*>
ethernet cfm domain none level <*level*>

Syntax Description

domain <*name*>	Specifies the MD's name. The name can be up to 42 characters in length.
level <*level*>	Specifies the MD's maintenance level. Range is **0** to **7**.
none	Specifies that the MD's name is not used to create the maintenance association ID (MAID).

Default Values

By default, no MDs exist.

Command History

Release 17.4	Command was introduced.

Functional Notes

This command not only creates and enables the MD, it also enters the MD Configuration mode. From the MD Configuration mode, maintenance associations (MAs) and maintenance endpoints (MEPs) can be configured. For more information on configuring MAs and MEPs, refer to the *Ethernet OAM CFM Command Set on page 4405*. When the **no** form of this command is used, the MD is deleted, as well as any MAs and MEPs defined with the domain.

The domain name serves two purposes. One is to provide a text label used in the device configuration to identify a particular domain, the other is to construct an MAID. The MAID is included in CFM continuity check messages (CCMs), and identifies the MA to which the transmitting MEP belongs. The MAID also allows MEPs receiving CCMs to detect CFM error conditions.

Because each MEP supported on an AOS device port or interface must be at a different MD level, each MEP on a particular port or interface will have to be configured on a separate MD.

For more information about Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates, enables, and enters the configuration mode of a MD named **Domain1**, created on level **6**:

(config)**#ethernet cfm domain Domain1 level 6**
(config-ecfm-domain)#

ethernet cfm log-changes

Use the **ethernet cfm log-changes** command to enable Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) warning messages on the AOS device. Warning messages are generated when remote maintenance endpoint (MEP) defects are detected. The **no** form of this command causes the warning messages to appear as debug messages.

Syntax Description

No subcommands.

Default Values

By default, warning messages are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information about Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables Ethernet OAM CFM warning messages:

(config)**#ethernet cfm log-changes**

ethernet flow-control-accept

Use the **ethernet flow-control-accept** command to include 802.3 media access control (MAC) control frames in the L2 discard counters when an Ethernet Virtual Circuit (EVC) map is configured to match L2CP traffic and discard all matched traffic. Depending on the EVC map configuration, the 802.3 MAC control frames are either counted by the L2 Discard Action counter or the L2 Discard counter when this feature is enabled (refer to the *Functional Notes* below). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R13.9.0	Command was introduced.

Functional Notes

In typical carrier Ethernet configurations, all Layer 2 incoming frames on the user network interface (UNI) port of a carrier Ethernet device are matched against the criteria specified in the evc-map configured on the UNI port. Frames that match the specified criteria are typically forwarded through on the associated EVC.

However, EVC maps can be configured to discard any frames matching the evc-map criteria. When the EVC map is configured to match L2CP traffic (using the command *match on page 3711*), as well as discard any matching traffic (using the command *connect discard on page 3710*), then all L2CP traffic is discarded. (Refer to the *Carrier Ethernet EVC Map Command Set on page 3705* for more information about the **connect discard** and **match** commands used in EVC map configuration).

Using the **ethernet flow-control-accept** command, in addition to an EVC map configured to discard L2CP traffic, allows 802.3 MAC control frames to be counted as part of the discarded traffic in the L2 Discard Action counter.

Using the **ethernet flow-control-accept** command in addition to EVC maps that are not configured to match L2CP traffic, specifies that the 802.3 MAC control frames are counted as part of the discarded traffic in the L2 Discard counter.

Usage Examples

The following example configure an EVC map, named **L2CP_Discard**, to discard all L2CP traffic, and then uses the **ethernet flow-control-accept** command to specify that 802.3 MAC control frames will also be counted in the L2 Discard Action counter:

(config)**#evc-map L2CP_Discard**
(config-evc-map L2CP_Discard)**#match l2cp**
(config-evc-map L2CP_Discard)**#connect uni gigabit-ethernet 0/3**
(config-evc-map L2CP_Discard)**#connect discard**
(config-evc-map L2CP_Discard)**#no ce-vlan-tpid**
(config-evc-map L2CP_Discard)**#no shutdown**
(config-evc-map L2CP_Discard)**#exit**
(config)**#ethernet flow-control-accept**

The following example configures an EVC map, named **L2CP_NoMatch**, that does not have L2CP traffic specified as matching criteria, and then uses the **ethernet flow-control-accept** command to specify that 802.3 MAC control frames are counted in the L2 Discard counter:

(config)**#evc-map L2CP_NoMatch**
(config-evc-map L2CP_NoMatch)**#connect uni gigabit-ethernet 0/3**
(config-evc-map L2CP_NoMatch)**#connect discard**
(config-evc-map L2CP_NoMatch)**#no ce-vlan-tpid**
(config-evc-map L2CP_NoMatch)**#no shutdown**
(config-evc-map L2CP_NoMatch)**#exit**
(config)**#ethernet flow-control-accept**

ethernet lmi

Use the **ethernet lmi** command to configure the Ethernet local management interface (E-LMI) polling parameters. Use the **no** form of this command to return the E-LMI polling parameters to the default value. Variations of this command include:

ethernet lmi n393 <*value*>
ethernet lmi t392 <*value*>
ethernet lmi t392 0

Syntax Description

n393 <*value*>	Configures the E-LMI operational polling status counter. Valid range is **2** to **10**.
t392 <*value*>	Configures the E-LMI polling timer in seconds. Valid range is **5** to **30** seconds.
t392 0	Disables the E-LMI polling timer.

Default Values

By default, the E-LMI polling status counter is set to **4**, and the polling timer is set to **15** seconds.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example configures the E-LMI polling status counter:

(config)**#ethernet lmi n393 8**

The following example disables the E-LMI polling timer:

(config)**#ethernet lmi t392 0**

ethernet loopback facility *<name> <slot>*

Use the **ethernet loopback facility** command to create a facility loopback object and enter the Facility MAC Swap Loopback Configuration mode. Use the **no** form of this command to delete the facility loopback object.

Syntax Description

<name>	Specifies the name of the facility loopback object.
<slot>	Specifies the slot identifier of the facility loopback object.

Default Values

No default values are necessary for this command.

Command History

Release R11.1.0	Command was introduced.

Functional Notes

In a facility media access control (MAC) swap loopback test, traffic is looped back upon ingressing the AOS unit. A flow ingressing the Metro Ethernet network (MEN) port interface is turned back toward that interface immediately upon entering the switch fabric. This loopback incorporates only the conditioning associated with the device's MEN port (shaping). Facility loopbacks are commonly used to validate round-trip data flow between a test head and a remote device's interface to the Ethernet backhaul. For more information regarding facility loopback objects and facility MAC swap loopback, refer to *Facility MAC Swap Loopback Command Set on page 3742*.

Usage Examples

The following example creates a facility loopback object named **FACILITY** and enters the Facility MAC Swap Loopback Configuration mode:

```
(config)#ethernet loopback facility FACILITY 0
Facility loopback "FACILITY" created
(config-eth-lbk-fac FACILITY 0)#
```


ethernet loopback system mac address

Use the **ethernet loopback system mac address** command to create a system loopback media access control (MAC) address that can be used for all MAC swap loopback tests. Use the **no** form of this command to delete the system loopback MAC address. Variations of this command include:

ethernet loopback system mac address *<mac address>*
ethernet loopback system mac address none

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
none	Specifies that the system loopback MAC address is not assigned.

Default Values

By default, no system loopback MAC address is defined.

Command History

Release R11.1.0	Command was introduced.

Functional Notes

In a loopback test, a signal is transmitted to a remote device, where it is returned (looped back) to the transmitting device. The transmitted and received signals can then be compared to prove circuit connectivity, isolate faults, and analyze characteristics of the data flow. Ethernet MAC swap loopback tests are analogous to traditional loopback tests employed in time division multiplexing (TDM) networks. However, in MAC swap loopbacks, the source MAC address and destination MAC addresses in the frame are swapped when the data is returned so that the incoming source and destination addresses become the outgoing destination and source addresses, respectively. This address swap is necessary because Ethernet address rules do not allow frames containing the same source MAC address to arrive from different ports on a device. For more information regarding facility loopback objects and facility MAC swap loopback, refer to *Facility MAC Swap Loopback Command Set on page 3742*.

Usage Examples

The following example configures the system loopback MAC address **00:A0:C8:00:00:01**::

(config)**#ethernet loopback system mac address 00:A0:C8:00:00:01**

ethernet loopback terminal *<name> <slot>*

Use the **ethernet loopback terminal** command to create a terminal loopback object and enter the Carrier Ethernet Terminal Loopback Configuration mode. Use the **no** form of this command to delete the terminal loopback object.

Syntax Description

<name>	Specifies the name of the terminal loopback object.
<slot>	Specifies the slot identifier of the terminal loopback object.

Default Values

No default values are necessary for this command.

Command History

Release R13.7.0	Command was introduced.

Functional Notes

In a Carrier Ethernet terminal loopback test, traffic is sent up-stream to a remote AOS device and then looped back just prior to egressing the remote AOS unit. A flow approaching the remote device's user network interface (UNI) port interface is turned back toward the switch fabric as close as possible to the UNI interface and returns traffic to the originating AOS device that is subject the same conditioning associated with the remote device's configured egress queue management and classification rules for down-stream traffic (such as Quality of Service (QoS) policers, shapers, matching criteria, and queues). Terminal loopbacks are commonly used to validate how a remote devices perform QoS on down-stream traffic by providing insight into rate limiting functionality on configured policers, traffic prioritization in egress queues, and traffic shaping as it is looped back towards the originating device.

For more information regarding terminal loopback objects and carrier Ethernet terminal loopback tests, refer to *Carrier Ethernet Terminal Loopback Command Set on page 3739*.

Usage Examples

The following example creates a terminal loopback object named **TERMINAL** and enters the Carrier Ethernet Terminal Loopback Configuration mode:

```
(config)#ethernet loopback terminal TERMINAL 0
Terminal loopback "TERMINAL" created
(config-eth-lbk-term TERMINAL 0)#
```


ethernet nni

Use the **ethernet nni** command to enable strict priority traffic management on the specified network-to-network interface (NNI). When enabled, all traffic, no matter the class, that is destined to the NNI is given a higher priority than traffic on all other user network interfaces (UNIs). Use the **no** form of this command disable strict priority traffic management on the specified NNI. Variations of this command include:

ethernet nni efm-group <*slot/group*>
ethernet nni gigabit-ethernet <*slot/port*>

Syntax Description

efm-group <*slot/group*>	Specifies an Ethernet in the first mile (EFM) group interface as the NNI on which strict priority traffic management is enabled. Valid group range is **1** to **1024**.
gigabit-ethernet <*slot/port*>	Specifies a Gigabit Ethernet interface as the NNI on which strict priority traffic management is enabled.

Default Values

By default, the NNI is not specified and strict priority traffic management is disabled.

Command History

Release R13.6.0	Command was introduced.

Usage Examples

The following example configures the EFM group **1/1** as the NNI with the highest priority traffic:

(config)**#ethernet nni efm-group 1/1**

ethernet s-tag-tpid <*data*>

Use the **ethernet s-tag-tpid** command to specify the Tag Protocol Identifier (TPID) used on all applied s-tags. Use the **no** form of this command to return to the default setting.

Syntax Description

<*data*>	Specifies a hex pattern to define the TPID. Valid range is **0x0800** to **0xFFFF**.

Default Values

By default, the TPID value is **8100**.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example specifies the TPID for s-tags as **88a8**:

(config)**#ethernet s-tag-tpid 88a8**

ethernet y1731 enable

Use the **ethernet y1731 enable** command to enable the Y.1731 subsystem. Use the **no** form of this command to disable the Y.1731 subsystem. Variations of this command include:

ethernet y1731 enable
ethernet y1731 enable down-mep md-level-check-filter

Syntax Description

down-mep md-level-check-filter	Optional. Enables Y.1731 frames received on a UNI port to be discarded if the MD level of the Y.1731 frame is less than or equal to the MEG level of the down MEP configured on the device.

Default Values

By default, the Y.1731 sub-system is disabled.

Command History

Release R10.10.0	Command was introduced.
Release R13.6.0	Command was expanded to include the **down-mep md-level-check-filter** parameter.

Usage Examples

The following example enables the Y.1731 subsystem:

(config)**#ethernet y1731 enable**

ethernet y1731 file-save consumption-limit

Use the **ethernet y1731 file-save consumption-limit** command to specify the maximum amount of memory that can be used to store Y.1731 performance monitoring log files. The limit specified must be larger than the space consumed by one performance monitoring file in order to allow the file to be written to memory. Use the **no** form of this command to return to the default value. Variations of this command include:

ethernet y1731 file-save consumption-limit frame-delay two-way <*memory*>
ethernet y1731 file-save consumption-limit frame-loss single-ended <*memory*>
ethernet y1731 file-save consumption-limit frame-loss synthetic single-ended <*memory*>

Syntax Description

frame-delay two-way <*memory*>	Specifies the maximum amount of memory in bytes used by two-way frame delay (ETH-DM) performance monitoring logs. Valid range is **1000** to **4294967295**.
frame-loss single-ended <*memory*>	Specifies the maximum amount of memory in bytes used by single-ended frame loss (ETH-LM) performance monitoring logs. Valid range is **1000** to **4294967295**.
frame-loss synthetic single-ended <*memory*>	Specifies the maximum amount of memory in bytes used by single-ended synthetic frame loss (ETH-SLM) performance monitoring logs. Valid range is **1000** to **4294967295**.

Default Values

By default, the maximum memory used by each performance monitoring log file type is **1000000** bytes.

Command History

Release 11.6.0	Command was introduced.

Functional Notes

By default, each time a new measurement interval occurs during a Y.1731 performance monitoring session, ETH-DM, ETH-LM, and ETH-SLM, the data from the previous interval is overwritten. The performance monitoring file save feature allows performance monitoring logs to be stored in memory in a series of hour-long log files. The unit records session data to the current log file at user-specified intervals. At the end of the user-specified log lifetime, the logs are rotated out in a first-in first-out fashion; the oldest files are deleted to make room for the new files. Each performance monitoring session type is stored in a separate file in the user-specified directory. The file is automatically named by the unit using the following format:

<*device serial*>**_<DM | LM | SLM>.Data_**<*date and time*>**.pm.xz[.current]**

Parameter	Description
<device serial>	Specifies the serial number of the unit.
DM	Specifies that the file is a single-ended (two-way) frame delay log.
LM	Specifies that the file is a single-ended frame loss log.
SLM	Specifies that the file is a single-ended synthetic frame loss log.
<date and time>	Specifes the date and time at which the log ends in the format **YYYY-MM-DD_hh.mm.ss**, for example: **2014-12-30_14:00:00**. This specifies the last time interval that the file will be written.
.pm.xz	Specifies the file extension of the log file.
.current	Appended to files that are still in use and could have data written to them.

The following example is a sample ETH-SLM file name that is no longer writable:

LBADTN340767_SLM.Data_2014-12-04_15.00.00.pm.xz

The following example is a sample ETH-LM file name of a file to which the unit is currently writing:

LBADTN340767_LM.Data_2014-12-04_15.00.00.pm.xz.current

If the file directory for the log files is changed, the files in the previous save directory will not be deleted for log rotation. Log rotation only occurs for files in the currently-specified save directory.

If any of the following conditions occur during a measurement interval, the measurement will be considered suspect, and it will be marked with a suspect flag:

- There is loss of continuity (LOC) during a measurement interval. If the LOC alarm is raised in the maintenance entity group end point (MEP) by continuity check messages (CCMs) during a measurement interval, the suspect flag will be raised for that measurement interval.
- The clock is adjusted by more than 10 seconds. If the system clock is adjusted by more than 10 seconds during a measurement interval, the suspect flag will be raised.
- The performance monitoring session is started during a measurement interval. If the session starts during a measurement interval (for example, a performance monitoring session is initiated at 3:00 with a measurement interval of 5 minutes, and the start time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The performance session is stopped during a measurement interval. If the session stops during a measurement interval (for example, a performance monitoring session was initiated at 3:00 with a measurement interval of 5 minutes, and the stop time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The Ethernet virtual circuit (EVC) status transitions to **Not Running** during a measurement interval. If the EVC over which the performance monitoring session is conducted transitions to a **Not Running** state during a measurement interval, the suspect flag will be raised for that measurement interval.
- The MEP transitions to an **Unavailable** or **Out of Service** state during a measurement interval. If the MEP goes to an **Unavailable** or **Out of Service** state during a measurement interval, the suspect flag will be raised for that measurement interval.

Usage Examples

The following example specifies that ETH-LM performance monitoring logs should use a maximum of **2000000** bytes:

(config)**#ethernet y1731 file-save consumption-limit frame-loss single-ended 2000000**

ethernet y1731 file-save directory flash <directory>

Use the **ethernet y1731 file-save directory flash** <*directory*> command to specify the directory used to store Y.1731 performance monitoring log files. Use the **no** form of this command to save performance monitoring log files in the default directory.

Syntax Description

<*directory*>	Specifies the name of the directory in which to store Y.1731 performance monitoring logs.

Default Values

By default, the Y.1731 performance monitoring log files are saved in the **y1731_pm_files** directory in **flash**.

Command History

Release 11.6.0	Command was introduced.

Functional Notes

By default, each time a new measurement interval occurs during a Y.1731 performance monitoring session, ETH-DM, ETH-LM, and ETH-SLM, the data from the previous interval is overwritten. The performance monitoring file save feature allows performance monitoring logs to be stored in memory in a series of hour-long log files. The unit records session data to the current log file at user-specified intervals. At the end of the user-specified log lifetime, the logs are rotated out in a first-in first-out fashion; the oldest files are deleted to make room for the new files. Each performance monitoring session type is stored in a separate file in the user-specified directory. The file is automatically named by the unit using the following format:

<*device serial*>**_<DM | LM | SLM>.Data_**<*date and time*>**.pm.xz[.current]**

Parameter	Description
<*device serial*>	Specifies the serial number of the unit.
DM	Specifies that the file is a single-ended (two-way) frame delay log.
LM	Specifies that the file is a single-ended frame loss log.
SLM	Specifies that the file is a single-ended synthetic frame loss log.
<*date and time*>	Specifes the date and time at which the log ends in the format **YYYY-MM-DD_hh.mm.ss**, for example: **2014-12-30_14:00:00**. This specifies the last time interval that the file will be written.
.pm.xz	Specifies the file extension of the log file.
.current	Appended to files that are still in use and could have data written to them.

The following example is a sample ETH-SLM file name that is no longer writable:

LBADTN340767_SLM.Data_2014-12-04_15.00.00.pm.xz

The following example is a sample ETH-LM file name of a file to which the unit is currently writing:

LBADTN340767_LM.Data_2014-12-04_15.00.00.pm.xz.current

If the file directory for the log files is changed, the files in the previous save directory will not be deleted for log rotation. Log rotation only occurs for files in the currently-specified save directory.

If any of the following conditions occur during a measurement interval, the measurement will be considered suspect, and it will be marked with a suspect flag:

- There is loss of continuity (LOC) during a measurement interval. If the LOC alarm is raised in the maintenance entity group end point (MEP) by continuity check messages (CCMs) during a measurement interval, the suspect flag will be raised for that measurement interval.
- The clock is adjusted by more than 10 seconds. If the system clock is adjusted by more than 10 seconds during a measurement interval, the suspect flag will be raised.
- The performance monitoring session is started during a measurement interval. If the session starts during a measurement interval (for example, a performance monitoring session is initiated at 3:00 with a measurement interval of 5 minutes, and the start time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The performance session is stopped during a measurement interval. If the session stops during a measurement interval (for example, a performance monitoring session was initiated at 3:00 with a measurement interval of 5 minutes, and the stop time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The Ethernet virtual circuit (EVC) status transitions to **Not Running** during a measurement interval. If the EVC over which the performance monitoring session is conducted transitions to a **Not Running** state during a measurement interval, the suspect flag will be raised for that measurement interval.
- The MEP transitions to an **Unavailable** or **Out of Service** state during a measurement interval. If the MEP goes to an **Unavailable** or **Out of Service** state during a measurement interval, the suspect flag will be raised for that measurement interval.

Usage Examples

The following example specifies that Y.1731 performance monitoring logs should be saved in the **y1731_logs** directory in **flash**:

(config)**#ethernet y1731 file-save directory flash y1731_logs**

ethernet y1731 file-save interval *<interval>*

Use the **ethernet y1731 file-save directory interval** *<interval>* command to specify the frequency with which Y.1731 performance monitoring data will be written to the log files. Use the **no** form of this command to return to the default value.

Syntax Description

<interval>	Specifies the frequency (in seconds) with which Y.1731 performance monitoring data is written to to the log files. Valid range is **300** to **3600** seconds.

Default Values

By default, data is written to the Y.1731 performance monitoring log files every **900** seconds (15 minutes).

Command History

Release 11.6.0	Command was introduced.

Functional Notes

By default, each time a new measurement interval occurs during a Y.1731 performance monitoring session, ETH-DM, ETH-LM, and ETH-SLM, the data from the previous interval is overwritten. The performance monitoring file save feature allows performance monitoring logs to be stored in memory in a series of hour-long log files. The unit records session data to the current log file at user-specified intervals. At the end of the user-specified log lifetime, the logs are rotated out in a first-in first-out fashion; the oldest files are deleted to make room for the new files. Each performance monitoring session type is stored in a separate file in the user-specified directory. The file is automatically named by the unit using the following format:

*<device serial>***_<DM | LM | SLM>.Data_***<date and time>***.pm.xz[.current]**

Parameter	Description
<device serial>	Specifies the serial number of the unit.
DM	Specifies that the file is a single-ended (two-way) frame delay log.
LM	Specifies that the file is a single-ended frame loss log.
SLM	Specifies that the file is a single-ended synthetic frame loss log.
<date and time>	Specifes the date and time at which the log ends in the format **YYYY-MM-DD_hh.mm.ss**, for example: **2014-12-30_14:00:00**. This specifies the last time interval that the file will be written.
.pm.xz	Specifies the file extension of the log file.
.current	Appended to files that are still in use and could have data written to them.

The following example is a sample ETH-SLM file name that is no longer writable:

LBADTN340767_SLM.Data_2014-12-04_15.00.00.pm.xz

The following example is a sample ETH-LM file name of a file to which the unit is currently writing:

LBADTN340767_LM.Data_2014-12-04_15.00.00.pm.xz.current

If the file directory for the log files is changed, the files in the previous save directory will not be deleted for log rotation. Log rotation only occurs for files in the currently-specified save directory.

If any of the following conditions occur during a measurement interval, the measurement will be considered suspect, and it will be marked with a suspect flag:

- There is loss of continuity (LOC) during a measurement interval. If the LOC alarm is raised in the maintenance entity group end point (MEP) by continuity check messages (CCMs) during a measurement interval, the suspect flag will be raised for that measurement interval.
- The clock is adjusted by more than 10 seconds. If the system clock is adjusted by more than 10 seconds during a measurement interval, the suspect flag will be raised.
- The performance monitoring session is started during a measurement interval. If the session starts during a measurement interval (for example, a performance monitoring session is initiated at 3:00 with a measurement interval of 5 minutes, and the start time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The performance session is stopped during a measurement interval. If the session stops during a measurement interval (for example, a performance monitoring session was initiated at 3:00 with a measurement interval of 5 minutes, and the stop time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The Ethernet virtual circuit (EVC) status transitions to **Not Running** during a measurement interval. If the EVC over which the performance monitoring session is conducted transitions to a **Not Running** state during a measurement interval, the suspect flag will be raised for that measurement interval.
- The MEP transitions to an **Unavailable** or **Out of Service** state during a measurement interval. If the MEP goes to an **Unavailable** or **Out of Service** state during a measurement interval, the suspect flag will be raised for that measurement interval.

Usage Examples

The following example specifies that data is written to the Y.1731 performance monitoring logs every **300** seconds (5 minutes):

(config)**#ethernet y1731 file-save interval 300**

ethernet y1731 file-save lifetime

Use the **ethernet y1731 file-save lifetime** command to specify the amount of time a performance monitoring log file will remain in memory before the is rotated out. The oldest file is deleted from memory when a new log file must be written. Use the **no** form to return to the default value. Variations of this command include:

ethernet y1731 file-save lifetime <*lifetime*>
ethernet y1731 file-save lifetime unlimited

Syntax Description

<*lifetime*>	Specifies the number of seconds that log files will be kept (as long as the consumption limit is not exceeded). Valid range is **3600** to **4294967295**.
unlimited	Specifies that logs will be kept indefinitely.

Default Values

By default, the Y.1731 performance monitoring log files have a lifetime of **86400** seconds.

Command History

Release 11.6.0	Command was introduced.

Functional Notes

By default, each time a new measurement interval occurs during a Y.1731 performance monitoring session, ETH-DM, ETH-LM, and ETH-SLM, the data from the previous interval is overwritten. The performance monitoring file save feature allows performance monitoring logs to be stored in memory in a series of hour-long log files. The unit records session data to the current log file at user-specified intervals. At the end of the user-specified log lifetime, the logs are rotated out in a first-in first-out fashion; the oldest files are deleted to make room for the new files. Each performance monitoring session type is stored in a separate file in the user-specified directory. The file is automatically named by the unit using the following format:

<*device serial*>**_<DM | LM | SLM>.Data_**<*date and time*>**.pm.xz[.current]**

Parameter	Description
<*device serial*>	Specifies the serial number of the unit.
DM	Specifies that the file is a single-ended (two-way) frame delay log.
LM	Specifies that the file is a single-ended frame loss log.
SLM	Specifies that the file is a single-ended synthetic frame loss log.
<*date and time*>	Specifes the date and time at which the log ends in the format **YYYY-MM-DD_hh.mm.ss**, for example: **2014-12-30_14:00:00**. This specifies the last time interval that the file will be written.
.pm.xz	Specifies the file extension of the log file.
.current	Appended to files that are still in use and could have data written to them.

The following example is a sample ETH-SLM file name that is no longer writable:

LBADTN340767_SLM.Data_2014-12-04_15.00.00.pm.xz

The following example is a sample ETH-LM file name of a file to which the unit is currently writing:

LBADTN340767_LM.Data_2014-12-04_15.00.00.pm.xz.current

If the file directory for the log files is changed, the files in the previous save directory will not be deleted for log rotation. Log rotation only occurs for files in the currently-specified save directory.

If any of the following conditions occur during a measurement interval, the measurement will be considered suspect, and it will be marked with a suspect flag:

- There is loss of continuity (LOC) during a measurement interval. If the LOC alarm is raised in the maintenance entity group end point (MEP) by continuity check messages (CCMs) during a measurement interval, the suspect flag will be raised for that measurement interval.
- The clock is adjusted by more than 10 seconds. If the system clock is adjusted by more than 10 seconds during a measurement interval, the suspect flag will be raised.
- The performance monitoring session is started during a measurement interval. If the session starts during a measurement interval (for example, a performance monitoring session is initiated at 3:00 with a measurement interval of 5 minutes, and the start time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The performance session is stopped during a measurement interval. If the session stops during a measurement interval (for example, a performance monitoring session was initiated at 3:00 with a measurement interval of 5 minutes, and the stop time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The Ethernet virtual circuit (EVC) status transitions to **Not Running** during a measurement interval. If the EVC over which the performance monitoring session is conducted transitions to a **Not Running** state during a measurement interval, the suspect flag will be raised for that measurement interval.
- The MEP transitions to an **Unavailable** or **Out of Service** state during a measurement interval. If the MEP goes to an **Unavailable** or **Out of Service** state during a measurement interval, the suspect flag will be raised for that measurement interval.

Usage Examples

The following example specifies that Y.1731 performance monitoring logs should have a lifetime of **604800** (one week):

(config)**#ethernet y1731 file-save lifetime 604800**

ethernet y1731 linktrace-cache

Use the **ethernet y1731 linktrace-cache** command to configure the Y.1731 subsystem's linktrace cache settings. Use the **no** form of this command to return to the default setting. Variations of this command include:

ethernet y1731 linktrace-cache hold-time <*minutes*>
ethernet y1731 linktrace-cache size <*value*>

Syntax Description

hold-time <*minutes*>	Configures how long linktrace replies are maintained in the linktrace cache. Valid range is **1** to **100** minutes.
size <*value*>	Configures the maximum number of entires maintained in the linktrace cache. Valid range is **10** to **500** entries.

Default Values

By default, linktrace replies are maintained in the linktrace cache for **33** minutes, and a maximum of **100** entries is maintained in the linktrace cache.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example configures the unit to maintain linktrace replies in the cache for **100** minutes :

(config)#**ethernet y1731 linktrace-cache hold-time 100**

ethernet y1731 meg

Use the **ethernet y1731 meg** command to create a Y.1731 maintenance entity group (MEG) and access the Y.1731 MEG Configuration mode. Use the **no** form of this command to remove the specified MEG. Variations of this command include:

ethernet y1731 meg char-string <*name*> **level** <*value*>
ethernet y1731 meg icc-umc <*name*> **level** <*value*>

Syntax Description

char-string <*name*>	Specifies a MEG name using a character string format. Maximum length is **45** ASCII characters.
icc-umc <*name*>	Specifies a MEG name using the ITU-CarrierCode Unique MEG ID Code MEG (ICC-UMC) format. Maximum length is **13** ASCII characters.
level <*value*>	Specifies the MEG level. Valid range is **0** to **7**.

Default Values

By default, no MEGs are configured.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example creates a MEG using the character string format with a MEG level of **1**:

(config)**#ethernet y1731 meg char-string meg1 level 1**

evc *<name>*

Use the **evc** command to create an Ethernet virtual connection (EVC) and enter the EVC configuration mode. Using the **no** form of this command removes the EVC from the AOS unit's configuration.

Syntax Description

<name>	Specifies the name for the EVC.

Default Values

By default, no EVCs are configured.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

The EVC connects two endpoints (for example, an Ethernet in the first mile (EFM) group and the Gigabit Ethernet interface) and passes Ethernet service frames though the endpoints. The EVCs prevent data transfer between subscriber sites that are not part of the same EVC, thus providing data privacy and security similar to a Frame Relay or an asynchronous transfer mode (ATM) permanent virtual circuit (PVC). EVCs are configured to be part of a bonding group (EFM group).

More information about the configuration of EVCs can be found in the *MEF EVC Command Set on page 3674*.

Usage Examples

The following example creates an EVC named **DATA** and enters the EVC configuration mode:

```
(config)#evc DATA
(config-evc-DATA)#
```


evc-map <*name*>

Use the **mef evc-map** command to create a Layer2/Layer 3 Ethernet virtual connection (EVC) map and enter the EVC Map Configuration mode. The EVC map is used to match traffic to a specific EVC using matching criteria similar to that of quality of service (QoS) matching. Using the **no** form of this command removes the EVC map from the AOS unit's configuration.

Syntax Description

<*name*>	Specifies the name of the EVC map.

Default Values

By default, no EVC maps are configured.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

Once an EVC map is created, it must be configured and applied to both an EVC and a user network interface (UNI). For more information about the configuration of EVC maps, refer to *MEF EVC Map Command Set on page 3678*.

Usage Examples

The following example creates the EVC map **Map1** and enters the EVC Map Configuration mode:

```
(config)#evc-map Map1
(config-evc-map-Map1)#
```


event-history on

Use the **event-history on** command to enable event logging for the AOS system. Event log messages will not be recorded unless this command has been issued (regardless of the **event-history priority** configured). The event log may be displayed using the **show event-history** command. Use the **no** form of this command to disable the event log.

Syntax Description

No subcommands.

Default Values

By default, the AOS event logging capabilities are disabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

The event history provides useful information regarding the status of the system and individual port states. Use the event history as a troubleshooting tool when identifying system issues. The following is a sample event history log.

#show event-history
Using 526 bytes
2002.07.12 15:34:01 T1.t1 1/1 Yellow
2002.07.12 15:34:01 INTERFACE_STATUS.t1 1/1 changed state to down.
2002.07.12 15:34:02 T1.t1 1/1 No Alarms
2002.07.12 15:34:02 INTERFACE_STATUS.t1 1/1 changed state to up.
2002.07.12 15:34:03 INTERFACE_STATUS.eth 0/1 changed state to up.
2002.07.12 15:34:10 OPERATING_SYSTEM Warm Start
2002.07.12 15:34:12 PPP.NEGOTIATION LCP up
2002.07.12 15:34:12 PPP.NEGOTIATION IPCP up

Usage Examples

The following example enables the AOS event logging feature:

(config)**#event-history on**

event-history priority

Use the **event-history priority** command to set the threshold for events stored in the event history. All events with the specified priority or higher will be kept for viewing in the local event log. The event log may be displayed using the **show event-history** command. Use the **no** form of this command to keep specified priorities from being logged. Variations of this command include:

event-history priority debug
event-history priority error
event-history priority fatal
event-history priority info
event-history priority notice
event-history priority warning

Syntax Description

debug	Logs subsystem debugging events.
error	Logs events with **error** and **fatal** priorities.
fatal	Logs only events with a **fatal** priority.
info	Logs all events.
notice	Logs events with **notice**, **warning**, **error**, and **fatal** priorities.
warning	Logs events with **warning**, **error**, and **fatal** priorities.

Default Values

By default, no event messages are logged to the event history.

Command History

Release 1.1	Command was introduced.
Release R10.1.0	Command was expanded to include the **debug** keyword.

Functional Notes

The event history provides useful information regarding the status of the system and individual port states. Use the event history as a troubleshooting tool when identifying system issues. The following is a sample event history log.

#show event-history
Using 526 bytes
2002.07.12 15:34:01 T1.t1 1/1 Yellow
2002.07.12 15:34:01 INTERFACE_STATUS.t1 1/1 changed state to down.
2002.07.12 15:34:02 T1.t1 1/1 No Alarms
2002.07.12 15:34:02 INTERFACE_STATUS.t1 1/1 changed state to up.
2002.07.12 15:34:03 INTERFACE_STATUS.eth 0/1 changed state to up.
2002.07.12 15:34:10 OPERATING_SYSTEM Warm Start
2002.07.12 15:34:12 PPP.NEGOTIATION LCP up
2002.07.12 15:34:12 PPP.NEGOTIATION IPCP up

Usage Examples

The following example logs all events to the event history:

(config)**#event-history priority info**

event-history size *<size>*

Use the **event-history size** command to change the event log size for the AOS system. Use the **no** form of this command to return to the default setting.

Syntax Description

<size>	Specifies the log size in kilobytes. The valid range is **6** to **256**.

Default Values

By default, the event log size is 6 kilobytes.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Event log messages will not be recorded unless the **event-history on** command has been issued (regardless of the **event-history priority** configured). The event log can be displayed using the **show event-history** command.

Usage Examples

The following example sets the event history log to 256 kilobytes:

(config)**#event-history size 256**

exception memory minimum <*value*>

Use the **exception memory minimum** command to initiate a reboot when the specified minimum amount of memory is no longer available. This ensures that adequate memory is available to store an exception report. Use the **no** form of this command to disable rebooting when the minimum memory limitation is violated.

*Executing the **exception memory minimum** command may cause the unit to reboot. Adtran recommends only using this command if advised by Adtran Technical Support.*

Syntax Description

<*value*>	Specifies the minimum amount of memory (in bytes) that must be free before a reboot occurs.

Default Values

By default, **exception memory minimum** is disabled.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example sets the exception memory minimum to **3** MB:

(config)**#exception memory minimum 30000000**

exception report

Use the **exception report** command to specify the name of the output file for the exception report. Use the **no** form of this command to return to the default setting. Variations of this command include:

exception report
exception report file-name <*filename*>

Syntax Description

file-name <*filename*>	Optional. Specifies a file name for the exception report other than the default file name.

Default Values

By default, the exception report file name is **exception report-yyyyMMddHHmmss**. (The yyyyMMddHHmmss will be automatically replaced with the actual year, month, day, hour, minutes, and seconds.)

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example specifies **example** as the name of the output file for an exception report:

(config)**#exception report file-name example**
(config)**#exit**
#exception report generate
Exception report generated.
#show flash
1744 startup-config
45676 example-20050708080537
#config t
(config)**#no exception report file-name**
(config)**#exit**
Appropriate commands must be issued to preserve configuration.
#exception report generate
Exception report generated.
#show flash
1744 startup-config
45676 example-20050708080537
45900 exception-report-20050708080552

ffe wildcard

Use the **ffe wildcard** command to enable RapidRoute flow bundling for all interfaces within an Internet Protocol (IP) address family. Use the **no** form of this command to disable RapidRoute flow bundling on all interfaces within an IP address family. Variations of this command include:

ip ffe wildcard
ipv6 ffe wildcard

Syntax Description

ip	Specifies that flow bundling is disabled on all interfaces within the IP version 4 (IPv4) address family.
ipv6	Specifies that flow bundling is disabled on all interfaces within the IP version 6 (IPv6) address family.

Default Values

RapidRoute flow bundling is enabled by default.

Command History

Release R11.10.1	Command was introduced.

Functional Notes

RapidRoute flow bundling is enabled and automatically activated on most AOS products. This command is typically used in the **no** form to disable flow bundling and all wildcards for all interfaces in a particular address family. This may be needed when flow bundling is interacting with another AOS feature and it needs to be disabled. Entering the command in regular form re-enables flow bundling for all interfaces in the specified address family.

Usage Examples

The following example disables RapidRoute flow bundling and wildcards for all interfaces in the IPv4 address family:

(config)**#no ip ffe wildcard**

filesystem throttle

Use the **filesystem throttle** command to enable File Transfer Protocol (FTP) throttling. Enabling this command limits the number of FTP sessions, the maximum number of large files open at one time, the size of the large files, and the number of open files that are smaller than the large file size. Use the **no** form of this command to disable FTP throttling.

Syntax Description

No subcommands.

Default Values

By default, FTP throttling is disabled.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

When FTP throttling is enabled, the following limits are imposed on FTP sessions:

Maximum FTP Sessions: 24
Large File Size: 30 MB
Maximum Number of Large Files Open: 2
Number of files less than Large File Size open for FTP: FTP Session limit (24)

When FTP throttling is disabled, the following limits are imposed on FTP sessions:

Maximum FTP Sessions: 100
Large File Size: unlimited
Maximum Number of Large Files Open: unlimited
Number of files less than Large File Size open for FTP: FTP Session limit (100)

Usage Examples

The following example enables FTP throttling:

(config)**#filesystem throttle**

ftp authentication *<listname>*

Use the **ftp authentication** command to specify that an authentication, authorization, and accounting (AAA) authentication method list is used by the AOS device's internal File Transfer Protocol (FTP) server for FTP authentication. AAA must be enabled to apply the method list to FTP authentication. Use the **no** form of this command to remove the authentication method list from FTP authentication.

Syntax Description

<listname>	Specifies the AAA authentication method list to apply to FTP authentication.

Default Values

By default, no AAA authentication method list is applied to FTP. If AAA is enabled (using the command *aaa on on page 1187*), but no list is assigned to FTP, FTP automatically uses the local user list for authentication.

Command History

Release 5.1	Command was introduced.

Functional Notes

AAA must be enabled for an authentication list to be applied to FTP authentication. For more information on enabling AAA, refer to the command *aaa on on page 1187*.

AAA authentication lists for use with FTP can be lists that control user login permissions or lists that control user Enable mode access permissions. These lists are created using the following commands: *aaa authentication login on page 1169* and *aaa authentication enable default on page 1165*.

For more information on AAA configuration, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example attaches the authentication method list **MyList** to the FTP server:

(config)**#ftp authentication MyList**

garp timer <*value*>

Use the **garp timer** command to adjust the timers used in all Generic Attribute Registration Protocol (GARP) applications (currently only GARP VLAN Registration Protocol (GVRP)) on the switch. Use the **no** form of this command to return to the default setting. Variations of this command include:

garp timer join <*value*>
garp timer leave <*value*>
garp timer leaveall <*value*>

Syntax Description

join <*value*>	Specifies the timer value (in milliseconds) between GARP application join messages.
leave <*value*>	Specifies the timer value (in milliseconds) between GARP application leave messages (must be at least three times longer than the join timer).
leaveall <*value*>	Specifies the timer value (in milliseconds) between GARP application leave all messages (must be greater than the leave timer).

Default Values

By default, the **join** timer is **200** milliseconds, the **leave** timer is **600** milliseconds, and the **leaveall** timer is **10000** milliseconds.

Command History

Release 8.1	Command was introduced.

Functional Notes

All devices communicating using GARP in the network need to have the same values for these timers. Changing these values is not recommended.

Usage Examples

The following example specifies the time (in milliseconds) between GARP application **leave all** messages:

(config)**#garp timer leaveall 20000**

global-policer warning

Use the **global-policer warning** command to enable virtual AOS (vAOS) global policer warning event generation for both rate usage and dropped packet messages. Use the **no** form of this command to disable the warning messages.

Syntax Description

No subcommands.

Default Values

By default, vAOS global policer event messages are enabled.

Command History

Release R12.1.0	Command was introduced.

Usage Examples

The following example disables vAOS global policer event messages:

(config)**#no global-policer warning**

global-policer warning threshold dropped-packets *<number>*

Use the **global-policer warning threshold dropped-packets** command to configure a threshold for generating a virtual AOS (vAOS) global policer dropped packets warning event. Use the **no** form of this command to return the dropped packet threshold to the default value.

Syntax Description

<number>	Specifies the dropped packet threshold for generating vAOS global policer warning messages. Valid range is **1** to **4294967295** packets.

Default Values

By default, a vAOS global policer warning message is generated when over **10000** packets are dropped during the five minute warning period.

Command History

Release R12.1.0	Command was introduced.

Functional Notes

When the number of packets dropped due to exceeding the vAOS licensed bandwidth exceeds the specified threshold during the five minute warning period, a warning message will be generated. This message can be useful in determining the cause of dropped packets in the network.

Usage Examples

The following example specifies that vAOS global policer warning messages are sent when more than **675000** packets are dropped during the five minute warning period:

(config)**#global-policer warning threshold dropped-packets 675000**

global-policer warning threshold rate-percent *<percent>*

Use the **global-policer warning threshold rate-percent** command to specify that when the virtual AOS (vAOS) actual traffic rate exceeds the specified percentage of the total licensed data rate during the warning period (five minutes), a warning message is generated. Use the **no** form of this command to return the rate percent threshold to the default value.

Syntax Description

<percent>	Specifies the percent threshold for generating vAOS global policer warning messages. Valid range is **1** to **99** percent.

Default Values

By default, vAOS global policer messages are generated when **90** percent of the total licensed data rate is exceeded within a five minute period.

Command History

Release R12.1.0	Command was introduced.

Functional Notes

Traffic is not actually dropped by the vAOS global policer when this threshold is exceeded unless the licensed bandwidth is exceeded. This warning message can be useful in determining if additional vAOS bandwidth should be purchased.

Usage Examples

The following example configures the vAOS data usage rate that generates a warning message as **75** percent:

(config)**#global-policer warning threshold rate-percent 75**

gvrp

Use the **gvrp** command to enable GARP VLAN Registration Protocol (GVRP) on the switch globally. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, GVRP is disabled.

Command History

Release 8.1	Command was introduced.

Functional Notes

Disabling GVRP globally will disable GVRP on all interfaces.

Usage Examples

The following example enables GVRP on the switch globally:

(config)**#gvrp**

hmr intercept

Use the **hmr intercept** command to configure the Session Initiation Protocol (SIP) header manipulation rules (HMR) intercept feature, and enter the HMR Intercept Configuration mode. Use the **no** form of this command to remove the HMR intercept feature configuration.

Syntax Description

No subcommands.

Default Values

By default, no HMR intercept policies exist, and the feature is disabled.

Command History

Release R12.4.0	Command was introduced.

Functional Notes

HMR intercept is a mechanism that allows standard HMR policies to be used to alter the flow of selected SIP requests. HMR intercept policies, when created and enabled, are given first access to inbound SIP requests. These policies can be used to generate a request response, block the processing of a request, or modify a request before other SIP agents within the device gain control of the request.

The HMR intercept policy's rules are evaluated to determine whether one or more rules match a given SIP request. If a match occurs, all rules that match within the policy are applied to the traffic in the same way that inbound or outbound HMR policies are applied. In addition, HMR intercept actions assigned to the intercept policy are applied to the SIP request.

For more information about the HMR intercept policy rules and actions, refer to the *HMR Intercept Command Set on page 4812*. For more information about SIP HMR, refer to the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enters the HMR Intercept Policy configuration mode:

```
(config)#hmr intercept
(config-hmr-intercept)#
```


hmr policy *<name>*

Use the **hmr policy** command to create a Session Initiation Protocol (SIP) header manipulation rule (HMR) policy and enter the policy's configuration mode. The HMR policy is a named collection of one or more HMR rule sets, and the policy is used to apply the rule sets to specific SIP traffic, SIP proxy user traffic, SIP proxy server traffic, or trunks. Use the **no** version of this command to remove the HMR policy.

Syntax Descriptions

<name>	Specifies the name of the HMR policy.

Default Values

By default, no HMR policies exist.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

SIP header manipulation is achieved by creating an HMR policy, a set of HMR rules, and applying those rules to the HMR policy. The policy is then applied to a SIP trunk, to all SIP traffic on the AOS device, to SIP traffic sent or received by a SIP proxy user, or to a SIP traffic sent or received by a SIP proxy server. The HMR policies can be applied to either inbound or outbound SIP traffic. For more information about configuring SIP HMR policies, refer to *HMR Command Set on page 4762* or the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the SIP HMR policy **MYPOLICY1**, and enters the policy's configuration mode:

```
(config)#hmr policy MYPOLICY1
(config-policy-MYPOLICY1)#
```


hmr rule-set *<name>*

Use the **hmr rule-set** command to create a Session Initiation Protocol (SIP) header manipulation rule (HMR) rule set. An HMR rule set is a named collection of one or more sequenced message rules used for SIP header and message manipulation. When a rule set is applied to a message, all matching message rules are processed in sequence. Use the **no** form of this command to remove the HMR rule set.

Syntax Description

<name>	Specifies the name of the HMR rule set. Names must be unique for each configured rule set.

Default Values

By default, no HMR rule sets are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

HMR rule sets are used to apply message rules to SIP traffic. These message rules are a collection of one or more SIP header commands, that determine the types of SIP headers to act upon, and the action to be taken. For more information about the configuration of SIP HMR rules and rule sets, refer to *HMR Command Set on page 4762* or the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the HMR rule set **SET1**, and enters the rule set's configuration mode:

```
(config)#hmr rule-set SET1
(config-rule-set-SET1)#
```


hmr set public-variable <*variable*> new-value <*pattern*>

Use the **hmr set public-variable** command to specify a public variable to be used with Session Initiation Protocol (SIP) header manipulation rule (HMR) configurations. Use the **no** form of this command to remove the public variable.

> NOTE *Public variables for SIP HMR can be set globally using this command, or from the HMR Message Rule Configuration Mode (refer to HMR Command Set on page 4762 for more information).*

Syntax Description

<variable>	Specifies the variable to be set.
<pattern>	Specifies the new value to be used by the variable. The pattern can be a regular expression or a text string.

Default Values

By default, no public variables are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

For more information about the creation and use of public variables in SIP HMR, refer to the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example sets the value of the public variable **paiTest**:

(config)**#hmr set public-variable paiTest new-value match**

host

Use the **host** command to define an Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) host name either for the default virtual routing and forwarding (VRF) or for a specified VRF instance. This allows you to statically enter host names and addresses in the host table. Use the **no** form of this command to remove the static entries. Variations of this command include:

host <*hostname*> <*ipv4 address*>
host <*hostname*> <*ipv6 address*>
host vrf <*name*> <*hostname*> <*ipv4 address*>
host vrf <*name*> <*hostname*> <*ipv6 address*>

Syntax Description

<*hostname*>	Defines the name of the host being added to the host table.
<*ipv4 address*>	Specifies the IPv4 address associated with the host name. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*ipv6 address*>	Specifies the IPv6 address associated with the host name. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
vrf <*name*>	Optional. Specifies a nondefault VRF instance on which to define the IPv4 or IPv6 host name. If no VRF instance is specified, the host name is defined on the default unnamed VRF instance.

Default Values

By default, there are no static hosts configured.

Command History

Release 3.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command was expanded to include the <*ipv6 address*> parameter. In addition, the command syntax was changed to remove the **ip** keyword for Adtran internetworking products.
Release R10.1.0	The command syntax was changed to remove the **ip** keyword for Adtran voice products.

Functional Notes

The host name can be any combination of numbers and letters as long as it is not a valid IPv4 or IPv6 address or does not exceed 256 characters.

VRF instances on AOS products allow a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example defines three static entries to the host table:

(config)**#host mac 10.2.0.2**
(config)**#host dal 172.38.7.12**
(config)**#host name1 2001:DB8:1::1**

hostname *<name>*

Use the **hostname** command to create a name used to identify the unit. This alphanumeric string should be used as a unique description for the unit. This string will be displayed in all prompts. Use the **no** form of this command to remove a host name.

Syntax Description

<name>	Identifies the unit using an alphanumeric string up to 32 characters.

Default Values

By default, the host name is **router**.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example creates a host name for the AOS device of **ATL_RTR** to identify the system as the Atlanta router:

(config)**#hostname ATL_RTR**

http authentication <*listname*>

Use the **http authentication** command to assign a specified authentication, authorization, and accounting (AAA) list to use in authentication to the AOS device's Hypertext Transfer Protocol (HTTP) or HTTP secure (HTTPS) server. AAA must be enabled (using the command *aaa on on page 1187*) before you can apply an AAA list to HTTP authentication. Use the **no** form of this command to remove the AAA list name from HTTP authentication.

Syntax Description

<*listname*>	Specifies the AAA list to use in authentication to the AOS device's HTTP/HTTPS server.

Default Values

By default, no HTTP/HTTPS authentication is configured.

Command History

Release 3.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Usage Examples

The following example assigns the AAA list **Mylist1** to HTTP authentication:

(config)**#http authentication Mylist1**

http ip access-class <*ipv4 acl name*> in

se the **http ip access-class in** command to restrict access to the Internet Protocol version 4 (IPv4) Hypertext Transfer Protocol (HTTP) server using the specified IPv4 access control list (ACL). Use the **no** form of this command to remove the IPv4 ACL from the HTTP connection. Variations of this command include:

http ip access-class <*ipv4 acl name*> **in**
http ip access-class <*ipv4 acl name*> **in any-vrf**
http ip access-class <*ipv4 acl name*> **in vrf** <*name*>

Syntax Description

<*ipv4 acl name*>	Specifies the previously configured IPv4 ACL to use for IPv4 HTTP access restriction.
in	Specifies that the ACL is applied to incoming IPv4 HTTP connections.
any-vrf	Optional. Allows incoming IPv4 HTTP connections from any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Allows incoming IPv4 HTTP connections from a specified VRF instance.

Default Values

By default, no IPv4 ACLs are applied to IPv4 HTTP connections.

Command History

Release 3.1	Command was introduced.
Release 18.3	Command syntax was changed to relocate the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to relocate the **ip** keyword for IPv6 support in Adtran voice products.
Release R10.7.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example specifies that IPv4 HTTP access is restricted by applying the previously configured IPv4 ACL (**MyIPv4ACL**):

(config)**#http ip access-class MyIPv4ACL in**

http ip secure-access-class <*ipv4 acl name*> in

Use the **http ip secure-access-class in** command to restrict access to the Internet Protocol version 4 (IPv4) Hypertext Transfer Protocol secure (HTTPS) server using the specified IPv4 access control list (ACL). Use the **no** form of this command to remove the IPv4 ACL from the HTTPS connection. Variations of this command include:

http ip secure-access-class <*ipv4 acl name*> **in**
http ip secure-access-class <*ipv4 acl name*> **in any-vrf**
http ip secure-access-class <*ipv4 acl name*> **in vrf** <*name*>

Syntax Description

<*ipv4 acl name*>	Specifies the previously configured IPv4 ACL to use for HTTPS access restriction.
in	Specifies that the ACL is applied to incoming IPv4 HTTPS connections.
any-vrf	Optional. Allows incoming IPv4 HTTPS connections from any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Allows incoming IPv4 HTTPS connections from a specified VRF instance.

Default Values

By default, no IPv4 ACLs are applied to HTTPS connections.

Command History

Release 3.1	Command was introduced.
Release 18.3	Command syntax was changed to relocate the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to relocate the **ip** keyword for IPv6 support in Adtran voice products.
Release R10.7.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example specifies that HTTPS access is restricted by applying the previously configured IPv4 ACL (**MyIPv4ACL**):

(config)**#http ip secure-access-class MyIPv4ACL in**

http ipv6 access-class <*ipv6 acl name*> in

Use the **http ipv6 access-class in** command to restrict access to the Internet Protocol version 6 (IPv6) Hypertext Transfer Protocol (HTTP) server using the specified IPv6 access control list (ACL). Use the **no** form of this command to remove the IPv6 ACL from the HTTP connection. Variations of this command include:

http ipv6 access-class <*ipv6 acl name*> **in**
http ipv6 access-class <*ipv6 acl name*> **in any-vrf**
http ipv6 access-class <*ipv6 acl name*> **in vrf** <*name*>

Syntax Description

<*ipv6 acl name*>	Specifies the previously configured IPv6 ACL to use for HTTP access restriction.
in	Specifies that the ACL is applied to incoming IPv6 HTTP connections.
any-vrf	Optional. Allows incoming IPv6 HTTP connections from any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Allows incoming IPv6 HTTP connections from a specified VRF instance.

Default Values

By default, no IPv6 ACLs are applied to HTTP connections.

Command History

Release 18.3	Command was introduced.
Release R10.7.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example specifies that HTTP access is restricted by applying the previously configured IPv6 ACL (**MyIPv6ACL**):

(config)**#http ipv6 access-class MyIPv6ACL in**

http ipv6 secure-access-class <*ipv6 acl name*> in

Use the **http ipv6 secure-access-class in** command to restrict access to the Internet Protocol version 6 (IPv6) Hypertext Transfer Protocol secure (HTTPS) server using the specified IPv6 access control list (ACL). Use the **no** form of this command to remove the IPv6 ACL from the HTTPS connection. Variations of this command include:

http ipv6 secure-access-class <*ipv6 acl name*> **in**
http ipv6 secure-access-class <*ipv6 acl name*> **in any-vrf**
http ipv6 secure-access-class <*ipv6 acl name*> **in vrf** <*name*>

Syntax Description

<*ipv6 acl name*>	Specifies the previously configured IPv6 ACL to use for HTTPS access restriction.
in	Specifies that the ACL is applied to incoming IPv6 HTTPS connections.
any-vrf	Optional. Allows incoming IPv6 HTTPS connections from any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Allows incoming IPv6 HTTPS connections from a specified VRF instance.

Default Values

By default, no IPv6 ACLs are applied to HTTPS connections.

Command History

Release 18.3	Command was introduced.
Release R10.7.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example specifies that HTTPS access is restricted by applying the previously configured IPv6 ACL (**MyIPv6ACL**):

(config)**#http ip secure-access-class MyIPv6ACL in**

http language

Use the **http language** command to specify the language of the Web-based Graphical User Interface (GUI) on the AOS device. Use the **no** form of this command to return the GUI language to the default value. Variations of this command include:

http language english
http language frenchcanadian
http language italian
http language latinamspanish
http language simplifiedchinese

Syntax Description

english	Specifies the GUI language is English.
frenchcanadian	Specifies the GUI language is French Canadian.
italian	Specifies the GUI language is Italian.
latinamspanish	Specifies the GUI language is Latin American Spanish.
simplifiedchinese	Specifies the GUI language is Simplified Chinese.

Default Values

By default, the GUI is displayed in English.

Command History

Release 3.1	Command was introduced.
Release 13.1	Command was expanded to include Italian.
Release 14.1	Command was expanded to include French Canadian, Latin American Spanish, and Simplified Chinese languages.
Release 18.3	Command syntax was changed to remove the **ip** keyword to support IPv6 in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Usage Examples

The following example specifies that the AOS GUI is displayed in French Canadian:

(config)**#http language frenchcanadian**

http report errors

Use the **http report errors** command to store a Hypertext Transfer Protocol (HTTP) error report on the unit's primary Flash memory when an HTTP server error occurs. The report is subsequently sent to the email address(es) specified by the command *logging email error-report address-list <email address> ; <email address> on page 1583*. Use the **no** form of this command to disable HTTP error reporting.

Syntax Description

No subcommands.

Default Values

By default, HTTP error reporting is enabled.

Command History

Release R10.8.0	Command was introduced.

Usage Examples

The following example enables HTTP error reporting:

(config)**#http report errors**

http secure-ciphersuite

Use the **http secure-ciphersuite** command to enable a secure sockets layer (SSL) cipher suite on Hypertext Transfer Protocol (HTTP) and HTTP secure (HTTPS) connections. Use the **no** form of this command to remove the SSL cipher suite configuration. Variations of this command include:

http secure-ciphersuite aes128-sha
http secure-ciphersuite aes256-sha
http secure-ciphersuite des-cbc-md5
http secure-ciphersuite des-cbc-sha
http secure-ciphersuite des-cbc3-md5
http secure-ciphersuite des-cbc3-sha
http secure-ciphersuite dhe-rsa-aes128-sha
http secure-ciphersuite dhe-rsa-aes256-sha
http secure-ciphersuite edh-rsa-des-cbc-sha
http secure-ciphersuite edh-rsa-des-cbc3-sha
http secure-ciphersuite rc4-md5
http secure-ciphersuite rc4-sha

Syntax Description

aes128-sha	Enables a secure sockets layer version 3.0 (SSLv3) cipher suite with the following properties: Key exchange algorithm (Kx) = Rivest, Sharmir, and Adleman (RSA) Authentication (Auth) = RSA Bulk encryption algorithm (E) = 128-bit Advanced Encryption Standard (AES) Hash function (Hash) = secure hash algorithm 1 (SHA-1)
aes256-sha	Enables an SSLv3 cipher suite with the following properties: Kx = RSA Auth = RSA E = 256-bit AES Hash = SHA-1
des-cbc-md5	Enables a secure sockets layer version 2.0 (SSLv2) cipher suite with the following properties: Kx = RSA Auth = RSA E = 56-bit Data Encryption Standard (DES) Hash = message-digest algorithm (MD5)
des-cbc-sha	Enables an SSLv3 cipher suite with the following properties: Kx = RSA Auth = RSA E = 56-bit DES Hash = SHA-1

des-cbc3-md5	Enables an SSLv2 cipher suite with the following properties: Kx = RSA Auth = RSA E = 168-bit Triple-DES (3DES) Hash = MD5
des-cbc3-sha	Enables an SSLv3 cipher suite with the following properties: Kx = RSA Auth = RSA E = 168-bit 3DES Hash = SHA-1
dhe-rsa-aes128-sha	Enables an SSLv3 cipher suite with the following properties: Kx = DH) Auth = RSA E = 128-bit AES Hash = SHA-1
dhe-rsa-aes256-sha	Enables an SSLv3 cipher suite with the following properties: Kx = DH Auth = RSA E = 256-bit AES Hash = SHA-1
edh-rsa-des-cbc-sha	Enables an SSLv3 cipher suite with the following properties: Kx = DH Auth = RSA E = 56-bit DES Hash = SHA-1
edh-rsa-des-cbc3-sha	Enables an SSLv3 cipher suite with the following properties: Kx = DH Auth = RSA E = 168-bit 3DES Hash = SHA-1
rc4-md5	Enables an SSLv2 or SSLv3 cipher suite with the following properties: Kx = RSA Auth = RSA E = 128-bit Rivest Cipher 4 (RC4) Hash = MD5
rc4-sha	Enables an SSLv3 cipher suite with the following properties: Kx = RSA Auth = RSA E = 128-bit RC4 Hash = SHA-1

Default Values

By default, no cipher suites are enabled.

Command History

Release 18.2	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Usage Examples

The following example enables the SSL cipher suite **rc4-sha** for HTTP connections:

(config)**#http secure-ciphersuite rc4-sha**

http secure-server

Use the **http secure-server** command to enable the Hypertext Transfer Protocol (HTTP) secure (HTTPS) server and specify the server use secure sockets layer (SSL) version 3. Use the **no** form of this command to disable the HTTP server. Variations of this command include:

http secure-server
http secure-server allow-tls1.0
http secure-server allow-tls1.0 allow-tls1.1
http secure-server allow-tls1.0 allow-tls1.1 allow-sslv3
http secure-server allow-tls1.0 allow-sslv3
http secure-server allow-tls1.1
http secure-server allow-tls1.1 allow-sslv3
http secure-server allow-sslv3
http secure-server <*TCP port*>
http secure-server <*TCP port*> **allow-tls1.0**
http secure-server <*TCP port*> **allow-tls1.0 allow-tls1.1**
http secure-server <*TCP port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
http secure-server <*TCP port*> **allow-tls1.0 allow-sslv3**
http secure-server <*TCP port*> **allow-tls1.1**
http secure-server <*TCP port*> **allow-tls1.1 allow-sslv3**
http secure-server <*TCP port*> **allow-sslv3**

Syntax Description

allow-tls1.0	Optional. Allows the server to use Transport Layer Security protocol version 1.0. If **allow-tls1.0** is enabled, SSLv3 can also optionally be enabled.
allow-tls1.1	Optional. Allows the server to use TLS protocol version 1.1. If allow-tls1.1 is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the server to use SSLv3. If SSLv3 is enabled, TLS version 1.0 is automatically enabled.
<*TCP port*>	Optional. Specifies an alternate Transmission Control Protocol (TCP) port to use for HTTPS connections.

Default Values

By default, the HTTP secure server is disabled. When the HTTP secure server is enabled, it uses SSLv3 by default.

Command History

Release 3.1	Command was introduced.
Release 17.6	Command was expanded to include the **allow-sslv2** parameter.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.

Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.
Release R12.3.0	Command was changed to remove the **allow-sslv2** keyword. In addition, the **allow-tls1.0** and **allow-sslv3** parameters were added.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example enables the HTTP secure server:

(config)**#http secure-server**

http server

Use the **http server** command to enable the Hypertext Transfer Protocol (HTTP) server on the AOS device. Enabling the server enables Web access to the AOS unit. Use the **no** form of this command to disable the HTTP server. Variations of this command include:

http server
http server <*TCP port*>

Syntax Description

<*TCP port*>	Optional. Specifies an alternate Transmission Control Protocol (TCP) port for the HTTP server.

Default Values

By default, the HTTP server is disabled.

Command History

Release 3.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Usage Examples

The following example enables the HTTP server:

(config)#**http server**

http session-limit <*number*>

Use the **http session-limit** command to set the maximum number of Hypertext Transfer Protocol (HTTP) or HTTP secure (HTTPS) sessions allowed on the AOS device. Use the **no** form of this command to return the maximum number of allowed sessions to the default value.

Syntax Description

<*number*>	Specifies the maximum number of allowed HTTP/HTTPS sessions. Valid range is **0** to **100** sessions.

Default Values

By default, up to **100** HTTP/HTTPS sessions are allowed.

Command History

Release 3.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Usage Examples

The following example limits the maximum number of allowed HTTP sessions to **75**:

(config)**#http session-limit 75**

http session-timeout <*value*>

Use the **http session-timeout** command to set the Hypertext Transfer Protocol (HTTP) or HTTP secure (HTTPS) session timeout value. Use the **no** form of this command to return the session timeout period to the default value.

Syntax Description

<*value*>	Specifies the HTTP/HTTPS session timeout period. Valid range is **10** to **86400** seconds.

Default Values

By default, the HTTP/HTTPS session times out after **600** seconds.

Command History

Release 3.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Usage Examples

The following example changes the HTTP session timeout period to **1500** seconds:

(config)**#http session-timeout 1500**

http source-interface <*interface*>

Use the **http source-interface** command to specify a source interface for Hypertext Transfer Protocol (HTTP) traffic originated by the AOS unit. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the configuration to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the configuration to the default unnamed VRF. The IP address of the specified interface will be used to source all HTTP traffic. Use the **no** form of this command if you do not wish to override the default source IP address. Variations of this command include:

http source-interface <*interface*>
http vrf <*name*> **source-interface** <*interface*>

This command pertains to the HTTP client and not the HTTP server.

Syntax Description

<*interface*>	Specifies the source interface for HTTP traffic. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip http source-interface ?** for a complete list of valid interfaces.
vrf <*name*>	Specifies the name of the VRF to which to configure the source interface.

Default Values

By default, no HTTP source interface is defined.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.
Release R10.7.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Functional Notes

This command allows you to override the Sender field in the IP packet. If you have multiple interfaces in your unit, changing the Sender tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for HTTP traffic:

(config)**#http source-interface loopback 1**

The following example configures the unit to use the **loopback 1** interface as the source IP for HTTP traffic on VRF RED:

(config)**#http vrf RED source-interface loopback 1**

hw-access-map <*name*>

Use the **hw-access-map** command to create and name a hardware access map. This command also enters the map's configuration mode. Using the **no** form of this command deletes the hardware access map.

For a complete list of all hardware access map configuration commands, refer to the *Hardware ACL and Access Map Command Set on page 4235*.

Syntax Description

<name>	Specifies the name of the hardware access map.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware access maps.

Command History

Release 17.6	Command was introduced.

Functional Notes

This command only creates an empty hardware access map, it does not configure it. For additional hardware access map configuration commands and configuration parameters, refer to the *Hardware ACL and Access Map Command Set on page 4235* or the *Hardware ACLs in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a hardware access map **Map1** and enters the hardware access map configuration mode:

```
(config)#hw-access-map Map1
(config-hw-access-map)#
```

Technology Review

Hardware access maps can only forward traffic. This action can be performed based on the criteria outlined in a single IP hardware access control list (ACL), a single medium access control (MAC) hardware ACL, or both. Like the hardware ACLs, the hardware access map will match traffic in top-down order.

If you configure the access map to reference a nonexistent IP or MAC hardware ACL, the ACL will be created. Note that this newly created ACL will have **permit any** as the default entry because no other entries are present.

Hardware access maps are not active until they are applied to a VLAN. For instructions on how to apply an access map to a VLAN, refer to *vlan <vlan id> on page 1889*.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

interface efm-group

Use the **interface efm-group** command to create an Ethernet in the first mile (EFM) group and enter the group's configuration. Use the **no** form of this command to remove the EFM group. Variations of this command include:

interface efm-group *<group number>*
interface efm-group *<slot/group>*
interface efm-group *<slot/group.subinterface id>*

Syntax Description

<group number>	Specifies the EFM group for use with Metro Ethernet Forum (MEF) configurations. Range is **1** to **1024**.
<slot/group>	Specifies the EFM group for use with carrier Ethernet Ethernet virtual connections (EVCs). The slot is the slot in which the interfaces bonded to the group reside. Group range is **1** to **1024**.
<slot/group.subinterface id>	Creates a Layer 3 subinterface on the Metro Ethernet network (MEN) port for Layer 3 services and enters the subinterface's configuration mode.

Default Values

By default, no EFM groups exist.

Command History

Release A4.01	Command was introduced.
Release R10.10.0	Command was expanded to include EFM group configuration for EVCs and Layer 3 subinterfaces on the MEN port.

Functional Notes

The EFM group is a logical interface that represents the EFM bonding group. The interfaces that are connected to the EFM group provide physical links to carry the bonded traffic. For more information about configuring the EFM group for MEF, refer to *MEF EFM Group Command Set on page 3599*. For more information about configuring the EFM group for EVCs or Layer 3 subinterfaces, refer to *Carrier Ethernet EFM Group Command Set on page 3691*.

Usage Examples

The following example creates EFM group **1** for MEF configurations and enters the group's configuration mode:

```
(config)#interface efm-group 1
(config-efm-group 1)#
```


interface mef-ethernet <*slot/port*>

Use the **interface mef-ethernet** command to enter the Metro Ethernet Forum (MEF) Ethernet Interface Configuration mode.

Syntax Description

<*slot/port*>	Specifies the slot and port of the MEF Ethernet interface.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Functional Notes

The MEF Ethernet interface is a virtual interface that provides connection between the Ethernet in the first mile (EFM) network interface module (NIM2) and the AOS unit.

If you are using 802.1q encapsulation, you must have a native VLAN MEF Ethernet subinterface configured for the EFM NIM2 to communicate with the AOS unit.

For more information about the MEF Ethernet interface, refer to *MEF Ethernet Interface on page 3604*. For more information about the configuration of EFM NIM2s and the MEF Ethernet interface, refer to the *Configuring EFM NIM2s and the MEF Ethernet Interface in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enters the configuration mode for MEF Ethernet interface in slot **1** port **1**:

(config)**#interface mef-ethernet 1/1**

interface range *<interface type> <slot/port>* - *<slot/port>*

Use the **interface range** command to enter configuration mode for a range of interfaces.

Syntax Description

<interface type>	Specifies the interface type (e.g., Ethernet, Gigabit Ethernet, etc.). Type **interface range ?** for a complete list of valid interfaces.
<slot/port>	Specifies the slot/port number of the first interface in the desired range of interfaces to be configured, followed by a hyphen (-) for consecutive ports or a comma (,) for nonconsecutive ports.
<slot/port>	Specifies the slot/port number of the last interface in the desired range of interfaces to be configured.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was expanded to include the foreign exchange office (FXO) range.
Release 14.1	Command was expanded to include the Gigabit Ethernet interfaces.
Release 18.2	Command was expanded to include the Single-Pair High-Speed Digital Subscriber Line (SHDSL) interface.
Release R10.10.0	Command was expanded to include the very high-speed digital subscriber line (VDSL), symmetric digial subscriber line (SDSL), and 10 gigabit switchport interfaces.

Functional Notes

All configuration changes made in this mode will apply to all interfaces in the range specified.

Usage Examples

The following example selects seven consecutive Ethernet ports for configuration:

(config)**#interface range eth 0/3-0/12**
(config-eth 0/3-12)#

The following example selects nonconsecutive Ethernet ports for configuration:

(config)**#interface range eth 0/14, 0/16, 0/18**
(config-eth 0/14, 0/16, 0/18)#

interface tunnel <*number*>

Use the **interface tunnel** command to create a tunnel interface and enter the tunnel's configuration mode. Use the **no** version of this command to remove the tunnel interface. Variations of this command include:

interface tunnel <*interface id*>
interface tunnel <*interface id*> **gre ip**
interface tunnel <*interface id*> **multipoint-gre ip**
interface tunnel <*interface id*> **vxlan**

Syntax Description

<interface id>	Specifies the tunnel's numerical label identifier. Valid range is **1** to **1024**.
gre ip	Specifies the tunnel is a point-to-point Generic Routing Encapsulation (GRE) tunnel, and that it is an Internet Protocol version 4 (IPv4) tunnel. This tunnel type encapsulates all IP traffic (both IPv4 and IPv6) in an IPv4/GRE delivery header.
multipoint-gre ip	Specifies the tunnel is a multipoint GRE tunnel. This tunnel type is used in Dynamic Multipoint Virtual Private Network (DMVPN) applications.
vxlan	Specifies the tunnel is a virtual extensible local area network (VxLAN) tunnel. This tunnel type is used to expand Layer 2 network segments across Layer 3 networks.

Default Values

By default, no tunnels are created.

Command History

Release R10.1.0	Command was introduced.
Release R11.9.0	Command was expanded to include the **multipoint-gre** parameter.
Release R13.1.0	Command was expanded to include **vxlan** parameter.

Functional Notes

The **interface tunnel gre ip** command replaces the **tunnel mode gre** command used from the tunnel interface in AOS firmware versions prior to R10.1.0. When the command is entered with the **gre ip** parameter, and a new tunnel interface is being created, the parameter creates the tunnel interface, specifies that all traffic (both IPv4 and IPv6) is encapsulated in an IPv4/GRE delivery header, and enters the tunnel's configuration mode. If the **gre ip** parameter is NOT used and the tunnel interface has NOT been previously created, an error is generated because the tunnel mode must be specified when creating a new tunnel interface. If the **gre ip** parameter is NOT used and the tunnel interface has been previously created, the command enters the tunnel's configuration mode. This logic also applies when using the **multipoint-gre ip** and **vxlan** parameters.

VxLAN tunnel implementation is point-to-point only since AOS does not currently support multicast VxLAN tunnels. VxLAN tunnel support is limited to IPv4 for underlay networks. However, IPv6 overlay networks can be created over IPv4 underlay networks.

Usage Examples

The following example creates a new tunnel interface, specifies the tunnel's mode as GRE, and enters the tunnel's configuration mode:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)#

ip access-list extended *<ipv4 acl name>*

Use the **ip access-list extended** command to create an empty Internet Protocol version 4 (IPv4) access control list (ACL) and enter the Extended ACL Configuration mode. Use the **no** form of this command to delete an extended ACL and all the entries contained in it.

For a complete list of all extended IPv4 ACL configuration commands, refer to the IPv4 Access Control List Command Set on page 4252.

Syntax Description

<ipv4 acl name>	Specifies the name of the IPv4 ACL.

Default Values

By default, all AOS security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.

Functional Notes

This command only creates an empty extended IPv4 ACL, it does not configure it. For additional extended ACL configuration commands and configuration parameters, refer to the *IPv4 Access Control List Command Set on page 4252*.

Usage Examples

The following example creates an extended IPv4 ACL **AllowIKfacility loopback objectE** and enters the Extended ACL Configuration mode:

(config)**#ip access-list extended AllowIKE**
(config-ext-nacl)#

Technology Review

IPv4 ACLs are used as packet selectors by different AOS IPv4 features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** ACL advances AOS to the next access policy entry. AOS provides two types of ACLs: standard and extended. Standard ACLs match based on the source of the packet. Extended ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

IPv4 ACLs cannot have the same name as IPv6 ACLs. If you are using both IPv4 and IPv6, you must have different ACLs for each IP version.

virtual routing and forwarding (VRF) on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

More information on IPv4 ACL, ACP, and AOS firewall configuration is available in the *IPv4 Firewall* configuration guide, located online at https://supportcommunity.adtran.com.

ip access-list standard *<ipv4 acl name>*

Use the **ip access-list standard** command to create an empty IPv4 access control list (ACL) and enter the Standard ACL Configuration mode. Use the **no** form of this command to delete an extended ACL and all the entries contained in it.

> NOTE *For a complete list of all standard IPv4 ACL configuration commands, refer to the IPv4 Access Control List Command Set on page 4252.*

Syntax Description

<ipv4 acl name>	Specifies the name of the IPv4 ACL.

Default Values

By default, all AOS security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.

Functional Notes

This command only creates an empty standard IPv4 ACL, it does not configure it. For additional standard IPv4 ACL configuration commands and configuration parameters, refer to the *IPv4 Access Control List Command Set on page 4252*.

Usage Examples

The following example creates a standard IPv4 ACL **AllowIKE** and enters the Standard ACL Configuration mode:

```
(config)#ip access-list standard AllowIKE
(config-std-nacl)#
```

Technology Review

IPv4 ACLs are used as packet selectors by different IPv4 AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** ACL advances AOS to the next access policy entry. AOS provides two types of ACLs: standard and extended. Standard ACLs match based on the source of the packet. Extended ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

IPv4 ACLs cannot have the same name as IPv6 ACLs. If you are using both IPv4 and IPv6, you must have different ACLs for each IP version.

Virtual routing and forwarding (VRF) on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

More information on ACL, ACP, and AOS firewall configuration is available in the *IPv4 Firewall* configuration guide, located online at https://supportcommunity.adtran.com.

ip classless

Use the **ip classless** command to forward classless packets to the best supernet route available. A classless packet is a packet addressed for delivery to a subnet of a network with no default network route.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

AOS products only function in classless mode. You cannot disable this feature.

Usage Examples

The following example enables the system to forward classless packets:

(config)**#ip classless**

ip crypto

Use the **ip crypto** command to enable AOS virtual private network (VPN) functionality and allow crypto maps to be added to the interfaces. Use the **no** form of this command to disable the VPN functionality. Variations of this command include:

ip crypto
ip crypto fast-failover

> *Disabling the AOS security features (using the **no ip crypto** command) does not affect VPN configuration settings (with the exception of the removal of all crypto maps from the interfaces). All other configuration parameters will remain intact, and VPN functionality will be disabled.*

Syntax Description

fast-failover	Optional. This setting is used when the same crypto map is applied to two different egress interfaces. It allows the quick deletion of Internet key exchange (IKE) and IPSec SAs when the default route policy class changes.

Default Values

By default, all AOS VPN functionality is disabled.

Command History

Release 4.1	Command was introduced.
Release 11.2	Command was expanded to include the **fast-failover** feature.

Functional Notes

VPN-related settings will not go into effect until you enable VPN functionality using the **ip crypto** command. AOS allows you to perform all VPN-related configuration prior to enabling **ip crypto**, with the exception of assigning a **crypto map** to an interface. The **no ip crypto** command removes all crypto maps from the interfaces. Enabling **ip crypto** enables the IKE server on User Datagram Protocol (UDP) Port 500. The **no** form of this command disables the IKE server on UDP Port 500.

Usage Examples

The following example enables VPN functionality:

(config)**#ip crypto**

ip crypto ffe

Use the **ip crypto ffe** command to enable the RapidRoute Engine for IP Security Protocol (IPSec) security associations (SAs). Use the **no** form of this command to disable the RapidRoute functionality for IPSec SAs. Variations of this command include:

ip crypto ffe
ip crypto ffe max-entries <*entries*>

Syntax Description

max-entries <*entries*>	Optional. Specifies the maximum number of entries per inbound (decrypting) IPSec SA. Valid range is from **1** to **8192**.

Default Values

By default, RapidRoute is not enabled for IPSec SAs. The default number of **max-entries** is **4096**.

Command History

Release 17.6	Command was introduced

Functional Notes

The RapidRoute Engine can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time can be specified by using the **max-entries** parameter.

Usage Examples

The following example enables RapidRoute for IPSec SAs and sets the maximum number of entries in the flow table to **50**:

(config)**#ip crypto ffe max entries 50**

ip crypto ipsec profile <*name*>

Use the **ip crypto ipsec profile** command to create a new crypto Internet Protocol security (IPsec) profile and enter the profile's configuration mode.Use the **no** form of this command to delete the IPsec profile.

Syntax Description

<*name*>	Specifies a unique, case-sensitive name for the IPsec profile to be created. Profile names cannot exceed **80** characters in length.

Default Values

By default, no IPsec profiles are configured.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

IPsec profiles can be applied to one or more tunnel interfaces.

An IPsec profile must have a transform set defined in order to function. Refer to the command *set transform-set on page 5268* for more information.

Usage Examples

The following example creates the IPsec profile **PROFILE1** and enters its configuration mode:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)#

ip crypto ipsec transform-set *<name> <parameters>*

Use the **ip crypto ipsec transform-set** command to define the transform configuration for securing data (e.g., esp-3des, esp-sha-hmac, etc.) using Internet Protocol version 4 (IPv4) IP security (IPsec). The transform set is then assigned to a crypto map using the map's **set transform-set** command. Refer to *set transform-set on page 5243*. Use the **no** form of this command to disable this feature.

The following additional subcommands are available once you have entered the Transform Set Configuration mode:

mode tunnel

Syntax Description

<name>	Specifies the name of the transform set. Names must be unique, and are specified in an alphanumeric string of up to **80** characters.	
<parameters>	Assigns a combination of up to three security algorithms to the set. Available security algorithms are as follows:	
	ah-md5-hmac	Authentication Header. Uses 16 byte \ and HMAC-MD5-96 authentication.
	ah-sha-hmac	Authentication Header. Uses 20 byte key and HMAC-SHA1-96 authentication.
	esp-des	Encapsulating Security Payload. Data encryption standard using cipher block chaining and an 8-byte key (DES-56-CBC).
	esp-3des	Encapsulating Security Payload. Data encryption standard using cipher block chaining and a 24-byte key (3DES-168-CBC).
	esp-aes-128-cbc	Encapsulating Security Payload. Advanced encryption standard using cipher block chaining and a 16-byte key.
	esp-aes-192-cbc	Encapsulating Security Payload. Advanced encryption standard using cipher block chaining and a 24-byte key.
	esp-aes-256-cbc	Encapsulating Security Payload. Advanced encryption standard using cipher block chaining and a 32-byte key.
	esp-null	Encapsulating Security Payload with no encryption.
	esp-md5-hmac	Encapsulating Security Payload. Uses 16-byte key and HMAC-MD5-96 authentication.
	esp-sha-hmac	Encapsulating Security Payload. Uses 20-byte key and HMAC-SHA1-96 authentication.
mode tunnel	Specifies the encapsulation mode for the transform set is datagram encapsulation (tunnel) mode.	

Default Values

By default, no IPv4 IPsec transform sets are configured.

Command History

Release 4.1	Command was introduced.
Release R10.7.0	Command syntax was changed to include the **ip** keyword.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets that contain specific security algorithms.

If no transform set is configured for a crypto map, the entry is incomplete and will have no effect on the system.

Usage Examples

The following example first creates a transform set (**Set1**) consisting of two security algorithms (up to three may be defined), and then assigns the transform set to a crypto map (**Map1**):

(config)**#ip crypto ipsec transform-set Set1 esp-3des esp-sha-hmac**
(cfg-crypto-trans)**#exit**
(config)**#ip crypto map Map1 1 ipsec-ike**
(config-crypto-map)**#set transform-set Set1**

ip crypto map

Use the **ip crypto map** command to define Internet Protocol version 4 (IPv4) crypto map entry names and numbers and to enter the associated mode (either Crypto Map Internet key exchange (IKE) or Crypto Map Manual). Use the **no** form of this command to disable this feature. Variations of this command include the following:

ip crypto map <*name*> <*index*>
ip crypto map <*name*> <*index*> **ipsec-ike**
ip crypto map <*name*> <*index*> **ipsec-manual**

Syntax Description

<*name*>	Specifies the name of the IPv4 crypto map entry. You can assign the same name to multiple crypto maps, as long as the map index numbers are unique.
<*index*>	Assigns a crypto map entry sequence number. Valid range is **0** to **65535**.
ipsec-ike	Specifies the crypto map IKE (refer to *Crypto Map IKE Command Set on page 5226*). This supports IPSec entries that will use IKE to negotiate keys.
ipsec-manual	Specifies the crypto map manual (refer to *IPv4 Crypto Map Manual Command Set on page 5244*). This supports manually configured IPSec entries.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release R10.7.0	Command syntax was changed to include the **ip** keyword.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets that contain specific security algorithms (refer to *data-call on page 1254*).

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list (ACL). An ACL is assigned to the crypto map using the **match address** command (refer to *ike-policy <number> on page 5230*).

If no transform set or access list is configured for a crypto map, the entry is incomplete and will have no effect on the system.

When you apply a crypto map to an interface (using the **crypto map** command within the interface's mode), you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Usage Examples

The following example creates a new IPv4 IPSec IKE crypto map called **testMap** with a map index of **10**:

(config)**#ip crypto map testMap 10 ipsec-ike**
(config-crypto-map)**#**

Technology Review

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of crypto map entries: **ipsec-manual** and **ipsec-ike**. Each entry is given an index that is used to sort the ordered list. When a nonsecured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the nonsecured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable security association (SA) exists, it is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists, and the crypto map entry is *respond only*, the packet is discarded.

When a secured packet arrives on an interface, its security parameter index (SPI) is used to look up an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

ip default-gateway *<ip address>*

Use the **ip default-gateway** command to specify a default gateway on a switch or on a router if (and only if) IP routing is NOT enabled on the router. Use the **ip route** command to add a default route to the route table when using IP routing functionality. Refer to *ip route on page 1447* for more information. Use the **no** form of this command to disable this feature.

Syntax Description

<ip address>	Specifies the default gateway IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there is no configured default gateway.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example disables IP routing on a router and configures a default gateway for **10.10.10.1**:

(config)**#no ip routing**
(config)**#ip default-gateway 10.10.10.1**

The following example specifies a default gateway for the management interface on a switch:

(config)**#ip default-gateway 10.10.10.1**

ip dhcp database local

Use the **ip dhcp database local** command to configure a Dynamic Host Configuration Protocol version 4 (DHCPv4) database agent with local bindings. Use the **no** form of this command to disable this option.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the hyphen and the **server** parameter for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **server** parameter for Adtran voice products.

Usage Examples

The following example configures the DHCPv4 database agent with local bindings:

(config)**#ip dhcp database local**

ip dhcp excluded-address

Use the **ip dhcp excluded-address** command to specify IPv4 addresses that cannot be assigned to Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured IPv4 address restriction. Variations of this command include:

ip dhcp excluded-address *<start ipv4 address>*
ip dhcp excluded-address *<start ipv4 address> <end ipv4 address>*
ip dhcp excluded-address vrf *<name> <start ipv4 address>*
ip dhcp excluded-address vrf *<name> <start ipv4 address> <end ipv4 address>*

Syntax Description

<start ipv4 address>	Specifies the lowest IPv4 address in the range OR a single IPv4 address to be excluded.
<end ipv4 address>	Optional. Specifies the highest IPv4 address in the range. This field is not required when specifying a single IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrf *<name>*	Optional. Specifies the nondefault virtual routing and forwarding (VRF) instance to which the IPv4 addresses are associated. If a VRF is not specified, the default unnamed VRF is assumed.

Default Values

By default, there are no excluded IPv4 addresses.

Command History

Release 2.1	Command was introduced.
Release 17.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran voice products.

Functional Notes

The AOS DHCPv4 server (by default) allows all IPv4 addresses for the DHCPv4 pool to be assigned to requesting clients. This command is used to ensure that the specified address or addresses are never assigned by the DHCPv4 server. When static-addressed hosts are present in the network, it is helpful to exclude the IPv4 addresses of the host from the DHCPv4 server IPv4 address pool. This will avoid IPv4 address conflict.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example excludes an IPv4 address of **172.22.5.100** and the range of IPv4 addresses **172.22.5.200** through **172.22.5.250**:

(config)**#ip dhcp excluded-address 172.22.5.100**
(config)**#ip dhcp excluded-address 172.22.5.200 172.22.5.250**

The following example excludes an IPv4 address of **172.22.5.100** and the range of IPv4 addresses **172.22.5.200** through **172.22.5.250** for the VRF instance named **RED**:

(config)**#ip dhcp excluded-address vrf RED 172.22.5.100**
(config)**#ip dhcp excluded-address vrf RED 172.22.5.200 172.22.5.250**

ip dhcp ping packets *<number>*

Use the **ip dhcp ping packets** command to specify the number of ping packets the Dynamic Host Configuration Protocol version 4 (DHCPv4) server will transmit before assigning an IPv4 address to a requesting DHCPv4 client. Transmitting ping packets verifies that no other hosts on the network are currently configured with the specified IPv4 address. Use the **no** form of this command to prevent the DHCPv4 server from using ping packets as part of the IPv4 address assignment process.

Syntax Description

<number>	Specifies the number of DHCPv4 ping packets sent on the network before assigning the IPv4 address to a requesting DHCPv4 client.

Default Values

By default, the number of DHCPv4 server ping packets is set at **2** packets.

Command History

Release 2.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran voice products.

Functional Notes

Before assigning an IPv4 address to a requesting client, the AOS DHCPv4 server transmits a ping packet on the network to verify there are no other network hosts already configured with the specified address. If the DHCPv4 server receives no reply, the IPv4 address is assigned to the requesting client and added to the DHCPv4 database as an assigned address. Configuring the **ip dhcp ping packets** command with a value of **0** prevents the DHCPv4 server from using ping packets as part of the IPv4 address assignment process.

Usage Examples

The following example configures the DHCPv4 server to transmit **4** ping packets before assigning an address:

(config)**#ip dhcp ping packets 4**

ip dhcp ping timeout <*value*>

Use the **ip dhcp ping timeout** command to specify the interval (in milliseconds) the Dynamic Host Configuration Protocol version 4 (DHCPv4) server will wait for a response to a transmitted DHCPv4 ping packet. The DHCPv4 server transmits ping packets before assigning an IPv4 address to a requesting DHCPv4 client. Transmitting ping packets verifies that no other hosts on the network are currently configured with the specified IPv4 address. Use the **no** form of this command to return to the default timeout interval.

Syntax Description

<*value*>	Specifies the number of milliseconds the DHCPv4 server will wait for a response to a transmitted DHCPv4 ping packet. Valid range is **1** to **1000** milliseconds.

Default Values

By default, the **ip dhcp ping timeout** is set to **500** milliseconds.

Command History

Release 2.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran voice products.

Functional Notes

Before assigning an IPv4 address to a requesting client, the AOS DHCPv4 server transmits a ping packet on the network to verify there are no other network hosts already configured with the specified address. If the DHCPv4 server receives no reply, the IPv4 address is assigned to the requesting client and added to the DHCPv4 database as an assigned address.

Usage Examples

The following example configures the DHCPv4 server to wait **900** milliseconds for a response to a transmitted DHCPv4 ping packet before considering the ping a failure:

(config)**#ip dhcp ping timeout 900**

ip dhcp pool <*name*>

Use the **ip dhcp pool** command to create a Dynamic Host Control Protocol version 4 (DHCPv4) server address pool and enter the pool's configuration mode. The server pool is used to define the information to be assigned to DHCPv4 clients by the DHCPv4 server. The pool chosen to serve a specific client's request is determined by the current pool selection algorithm. Refer to the *DHCPv4 Pool Command Set on page 4336* for more information.

Syntax Description

<name>	Specifies the name of the DHCPv4 server address pool using an alphanumeric string (up to 32 characters in length).

Default Values

By default, there are no configured DHCPv4 address pools.

Command History

Release 2.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the hyphen and the **server** keyword in Adtran voice products.

Functional Notes

Use the **ip dhcp pool** command to create multiple DHCPv4 server address pools for various segments of the network. Multiple address pools can be created to service different segments of the network with tailored configurations.

Usage Examples

The following example creates a DHCPv4 server address pool (labeled **SALES**) and enters the DHCPv4 server pool's configuration mode:

```
(config)#ip dhcp pool SALES
(config-dhcp)#
```


ip ffe limit exceptions *<value>*

Use the **ip ffe limit exceptions** command to specify a limit to the number of unhandled Internet Protocol version 4 (IPv4) fast forwarding engine (FFE) exception packets allowed at any given time by the RapidRoute feature. Use the **no** form of this command to return the limit to the default value.

Syntax Description

<value>	Specifies the maximum number of unhandled FFE exception packets allowed at a given time. Valid range is **1** to **1024**.

Default Values

By default, no more than **128** exception packets are allowed.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

Exception packets are any packets that RapidRoute cannot handle, for example, traffic that matches ineligible entries, fragmented packets, packets with header errors, or the first packet in a given traffic flow that is used to build an FFE entry. Once the limit of unhandled FFE exception packets is reached, subsequent exception packets are dropped until the previously unhandled exceptions are resolved.

Usage Examples

The following example specifies the maximum number of IPv4 exception packets allowed by RapidRoute are **200**:

(config)**#ip ffe limit exceptions 200**

ip ffe max-entries *<value>*

Use the **ip ffe max-entries** command to specify a global limit to the number of Internet Protocol version 4 (IPv4) fast forwarding engine (FFE) entries allowed at any given time by the RapidRoute feature. Use the **no** form of this command to return to the default value.

Issuing this command will cause all RapidRoute entries to be cleared from the unit.

Syntax Description

<value>	Specifies the total number of RapidRoute entries for all interfaces. Valid range is **1** to **500000**.

Default Values

By default, the **ip ffe max-entries** is set to **16384**.

Command History

Release 13.1	Command was introduced.
Release R10.4.0	Command was changed to include up to **500000** entries.

Usage Examples

The following example sets the total maximum number of IPv4 RapidRoute entries to **500**:

(config)**#ip ffe max-entries 500**

ip ffe timeout

Use the **ip ffe timeout** command to set the time to live (TTL) for Internet Protocol version 4 (IPv4) RapidRoute fast forwarding engine (FFE) entries based on their IPv4 protocol. Use the **no** form of this command to return to the default value. Variations of this command include:

ip ffe timeout ah <*max timeout*>
ip ffe timeout ah <*max timeout*> <*inactive timeout*>
ip ffe timeout esp <*max timeout*>
ip ffe timeout esp <*max timeout*> <*inactive timeout*>
ip ffe timeout gre <*max timeout*>
ip ffe timeout gre <*max timeout*> <*inactive timeout*>
ip ffe timeout icmp <*max timeout*>
ip ffe timeout icmp <*max timeout*> <*inactive timeout*>
ip ffe timeout other <*max timeout*>
ip ffe timeout other <*max timeout*> <*inactive timeout*>
ip ffe timeout tcp <*max timeout*>
ip ffe timeout tcp <*max timeout*> <*inactive timeout*>
ip ffe timeout udp <*max timeout*>
ip ffe timeout udp <*max timeout*> <*inactive timeout*>

Syntax Description

ah	Specifies timeout values in seconds for Authentication Header (AH) Protocol.
esp	Specifies timeout values in seconds for Encapsulating Security Payload (ESP) Protocol.
gre	Specified timeout values in seconds for Generic Route Encapsulation (GRE) Protocol.
icmp	Specifies timeout values in seconds for Internet Control Message Protocol (ICMP).
other	Specifies timeout values in seconds for all protocols not listed.
tcp	Specifies timeout values in seconds for Transmission Control Protocol (TCP).
udp	Specifies timeout values in seconds for User Datagram Protocol (UDP).
<*max timeout*>	Specifies maximum age timeout in seconds. This is the maximum amount of time an entry will be kept in the RapidRoute table regardless of activity. Valid range is **60** to **86400** seconds.
<*inactive timeout*>	Optional. Specifies idle timeout in seconds. This is the amount of time an entry will remain in the RapidRoute table with no additional activity. Valid range is **10** to **86400** seconds.

Default Values

By default, the maximum age timeouts are set to **1800** seconds and the inactive timeouts are set to **15** seconds.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the **gre** parameter.

Usage Examples

The following example sets the time to live for IPv4 RapidRoute entries of TCP packets to **1000** seconds.

(config)**#ip ffe timeout tcp 1000**

ip firewall

Use the **ip firewall** command to enable Internet Protocol version 4 (IPv4) AOS security features, including IPv4 access control policies (ACPs) and lists (ACLs), network address translation (NAT), and the stateful inspection firewall. Use the **no** form of this command to disable the security functionality.

*Disabling the AOS IPv4 security features (using the **no ip firewall** command) does not affect security configuration. All configuration parameters will remain intact, but no security data processing will be attempted.*

*For information regarding the use of open shortest path first (OSPF) with **ip firewall** enabled, refer to the **Functional Notes** for router ospf <process id> on page 1690.*

*Regarding the use of Internet key exchange (IKE) negotiation for virtual private network (VPN) with **ip firewall** enabled, there can be up to six channel groups with 2 to 8 interfaces per group. Dynamic protocols are not yet supported (only static). A physical interface can be a member of only one channel group.*

Syntax Description

No subcommands.

Default Values

By default, all AOS IPv4 security features are disabled.

Command History

Release 2.1	Command was introduced.

Functional Notes

This command enables firewall processing for all interfaces with a configured policy class. Firewall processing consists of the following functions:

Attack Protection: Detects and discards traffic that matches profiles of known networking exploits or attacks.

Session Initiation Control: Allows only sessions that match traffic patterns permitted by ACPs to be initiated through the router.

Ongoing Session Monitoring and Processing: Each session that has been allowed through the router is monitored for any irregularities that match patterns of known attacks or exploits. This traffic will be dropped. Also, if NAT is configured, the firewall modifies all traffic associated with the session according to the translation rules defined in NAT access policies. Finally, if sessions are inactive for a user-specified amount of time, the session will be closed by the firewall.

Application-Specific Processing: Certain applications need special handling to work correctly in the presence of a firewall. AOS uses application-level gateways (ALGs) for these applications.

AOS includes several security features to provide controlled access to your network. The following features are available when security is enabled (using the **ip firewall** command):

1. Stateful Inspection Firewall

AOS (and your unit) act as an ALG and employ a stateful inspection firewall that protects an organization's network from common cyber attacks, including Transmission Control Protocol (TCP) syn-flooding, IP spoofing, Internet Control Message Protocol (ICMP) redirect, land attacks, ping-of-death, and IP reassembly problems. In addition, further security is added with use of NAT and port address translation (PAT) capability.

2. IPv4 Access Policies

AOS IPv4 ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each ACP consists of an action (**allow**, **discard**, **nat**) and a selector (access control list (ACL)). In a sense, the ACPs answer the question, “What should I do?” while the ACLs answer the question, “On which packets?”

When packets are received on an interface with an ACP applied, the ACP is used to determine whether the data is processed or discarded. Both ACLs and ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed. The ACP has an implicit **discard** at the end of the list. Typically, the most specific entries should be at the top and the most general at the bottom.

3. IPv4 Access Lists

IPv4 ACLs are used as packet selectors by ACPs. They must be assigned to an ACP in order to be active. ACLs are composed of an ordered list of entries. Each entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** action is used to allow packets (meeting the specified pattern) to enter the router system. A **deny** action is used to disregard packets (that do not match the pattern) and proceed to the next entry on the ACP. The ACL has an implicit **deny** at the end of the list.

The AOS provides two types of ACLs: **standard** and **extended**. A **standard** ACL allows source IP address packet patterns only. An **extended** ACL may specify patterns using most fields in the IP header and the TCP or User Datagram Protocol (UDP) header.

Usage Examples

The following example enables the AOS IPv4 security features:

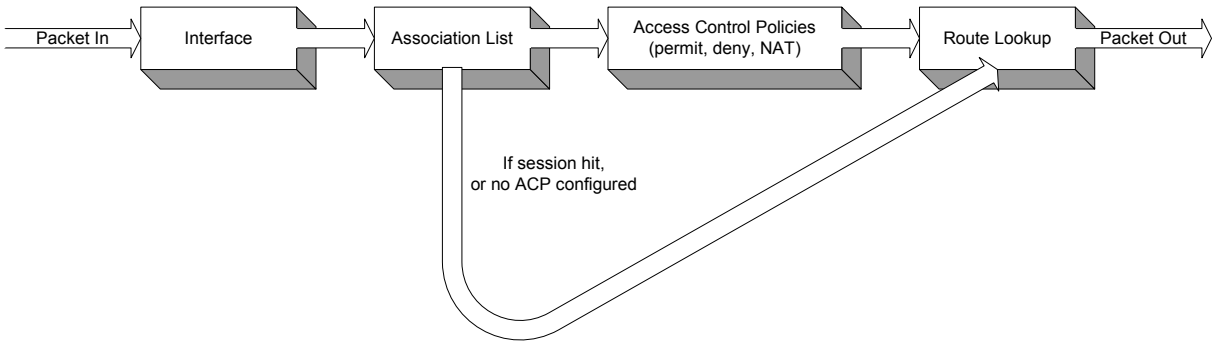
(config)**#ip firewall**

Technology Review

Concepts: IPv4 access control using the AOS firewall has two fundamental parts: ACLs and ACPs. ACLs are used as packet selectors by other AOS systems; by themselves they do nothing. ACPs consist of a selector (ACL) and an action (**allow**, **discard**, **nat**). ACPs integrate both **allow** and **discard** policies with NAT. ACPs have no effect until they are assigned to a network interface.

Both ACLs and ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed.

Packet Flow:



Case 1: Packets from interfaces with a configured policy class to any other interface

IPv4 ACPs are applied when packets are received on an interface. If an interface has not been assigned a policy class, by default it will allow all received traffic to pass through. If an interface has been assigned a policy class, but the firewall has not been enabled with the **ip firewall** command, traffic will flow normally from this interface with no firewall processing.

Case 2: Packets that travel in and out a single interface with a configured policy class

These packets are processed through the IPv4 ACPs as if they are destined for another interface (identical to Case 1).

Case 3: Packets from interfaces without a configured policy class to interfaces with one policy class

These packets are routed normally and are not processed by the IPv4 firewall. The **ip firewall** command has no effect on this traffic.

Case 4: Packets from interfaces without a configured policy class to other interfaces without a configured policy class

This IPv4 traffic is routed normally. The **ip firewall** command has no effect on this traffic.

Attack Protection:

When the **ip firewall** command is enabled, IPv4 firewall attack protection is enabled. AOS blocks traffic (matching patterns of known networking exploits) from traveling through the device. For some of these attacks, the user may manually disable checking/blocking while other attack checks are always on anytime the firewall is enabled.

The table (on the following pages) outlines the types of IPv4 traffic discarded by the firewall attack protection engine. Many attacks use similar invalid traffic patterns; therefore, attacks other than the examples listed below may also be blocked by the firewall. To determine if a specific attack is blocked by the AOS firewall, please contact Adtran technical support.

Invalid IPv4 Traffic Pattern	Manually Enabled?	AOS Firewall Response	Common Attacks
Larger than allowed packets	No	Any packets that are longer than those defined by standards will be dropped.	Ping of Death
Fragmented IP packets that produce errors when attempting to reassemble	No	The firewall intercepts all fragments for an IP packet and attempts to reassemble them before forwarding to destination. If any problems or errors are found during reassembly, the fragments are dropped.	SynDrop, TearDrop, OpenTear, Nestea, Targa, Newtear, Bonk, Boink
Smurf Attack	No	The firewall will drop any ping responses that are not part of an active session.	Smurf Attack
IP Spoofing	No	The firewall will drop any packets with a source IP address that appears to be spoofed. The IP route table is used to determine if a path to the source address is known (out of the interface from which the packet was received). For example, if a packet with a source IP address of 10.10.10.1 is received on interface fr 1.16 and no route to 10.10.10.1 (through interface fr 1.16) exists in the route table, the packet is dropped.	IP Spoofing
ICMP Control Message Floods and Attacks	No	The following types of ICMP packets are allowed through the firewall: echo, echo-reply, TTL expired, dest. Unreachable, and quench. These ICMP messages are only allowed if they appear to be in response to a valid session. All others are discarded.	Twinge
Attacks that send TCP URG packets	Yes	Any TCP packets that have the URG flag set are discarded by the firewall.	Winnuke, TCP XMAS Scan
Falsified IP Header Attacks	No	The firewall verifies that the packet's actual length matches the length indicated in the IP header. If it does not, the packet is dropped.	Jolt/Jolt2

Invalid IPv4 Traffic Pattern	Manually Enabled?	AOS Firewall Response	Common Attacks
Echo	No	All UDP echo packets are discarded by the firewall.	Char Gen
Land Attack	No	Any packets with the same source and destination IP addresses are discarded.	Land Attack
Broadcast Source IP	No	Packets with a broadcast source IP address are discarded.	
Invalid TCP Initiation Requests	No	TCP SYN packets that have ack, urg rst, or fin flags set are discarded.	
Invalid TCP Segment Number	No	The sequence numbers for every active TCP session are maintained in the firewall session database. If the firewall received a segment with an unexpected (or invalid) sequence number, the packet is dropped.	
IP Source Route Option	No	All IP packets containing the IP source route option are dropped.	

Application-Specific Processing

The following applications and protocols require special processing to operate concurrently with IPv4 NAT/firewall functionality. The AOS IPv4 firewall includes ALGs for handling these applications and protocols:

AOL Instant Messenger (AIM®)
VPN ALGS: ESP and IKE
FTP
H.323: H.245 Q.931 ASN1 PER decoding and Encoding
ICQ®
IRC
Microsoft® Games
Net2Phone
PPTP
Quake®
Real-Time Streaming Protocol
SMTP
HTTP
CUseeme
SIP
L2TP
PcAnywhere™
SQL
Microsoft Gaming Zone

To determine if a specific application requires special processing, contact Adtran technical support at www.adtran.com.

ip firewall alg

Use the **ip firewall alg** command to enable the Internet Protocol version 4 (IPv4) application-level gateway (ALG) for a particular application. Use the **no** form of this command to disable ALG for the application.

Variations of this command applicable for nonvoice capable Adtran products include the following:

ip firewall alg ftp
ip firewall alg h323
ip firewall alg h323 timeout <*number*>
ip firewall alg msn
ip firewall alg mszone
ip firewall alg pptp
ip firewall alg rtsp
ip firewall alg sip

Variations of this command applicable for voice capable Adtran products include the following:

ip firewall alg ftp
ip firewall alg h323
ip firewall alg h323 timeout <*number*>
ip firewall alg msn
ip firewall alg mszone
ip firewall alg pptp
p firewall alg rtsp

The AOS IPv4 firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

ftp	Enables the File Transfer Protocol (FTP) ALG.
h323	Enables the H.323 ALG. H.323 is a protocol that sets standards for multimedia communications over packet-switched networks, allowing dissimilar communication devices to communicate with each other via a standard communication protocol.
h323 timeout <*number*>	Optional. Allows the configuration of the timeout for the policy-session that controls the H.323 call, and specifies the length of time before the H.323 call is terminated after a timeout. Range is **1** to **4294967295** seconds.
msn	Enables the Microsoft Service Network (MSN) ALG.
mszone	Enables the MSZONE ALG.
pptp	Enables the PPTP ALG.
rtsp	Enables the Real Time Streaming Protocol (RTSP) ALG.

sip	Enables the Session Initiation Protocol (SIP) ALG. This ALG is only used in Adtran router and switch products, not voice products.

Default Values

By default, all AOS IPv4 security features are disabled until the IPv4 firewall is enabled. By default, the ALG for FTP, PPTP, RTSP, and SIP are enabled. Conversely, the ALG for MSN, MSZONE, and H.323 are disabled by default. There are no SIP ALGs present on voice capable Adtran products. By default, the timeout value for H.323 is set for 8 hours.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include H.323.
Release 14.1	Command was expanded to include MSN.
Release 15.1	Command was expanded to include H.323 timeout feature.
Release 17.4	Command was expanded to include MSZONE.
Release R10.1.0	Command was expanded to include RTSP.

Functional Notes

Enabling the ALG for a specific protocol gives the firewall additional information about that complex protocol and causes the firewall to perform additional processing for packets of that protocol. When the ALG is disabled, the firewall treats the complex protocol as any other simple protocol. The firewall needs no special knowledge to work well with simple protocols.

Disabling the IP firewall ALG may cause the firewall to block some of the traffic for the specified protocol.

Microsoft Service Network (MSN) ALG Information

In some instances where the firewall is enabled and traffic is source NATed through the unit, some features of MSN's instant messenger program will not work (i.e., file sharing, direct connection, etc.). Enabling the MSN ALG allows the firewall to inspect the MSN messaging protocol to allow some of these features to work through network address translation (NAT). If the traffic is not NATed, then this ALG is not required and should be disabled.

Session Initiation Protocol (SIP) ALG Information

By default, the AOS SIP ALG is enabled. This ALG allows the firewall to examine the ALL SIP packets it identifies and maintain knowledge of SIP transmissions on the network based on the SIP header.

Usage Examples

The following example disables ALG for FTP:

(config)**#no ip firewall alg ftp**

The following example enables ALG for MSN:

(config)**#ip firewall alg msn**

Technology Review

SIP is one protocol in a suite of protocols that was designed to replace H.323 for IP telephony. SIP operates in Layer 7 of the OSI model (application level) to create, modify, and terminate sessions between nodes. SIP not only provides recommendations for IP telephony, but multimedia distribution and conferences as well. SIP version 1.0 was defined in RFC 2453, and was refined to SIP version 2.0 in RFC 3261.

SIP operations occur between SIP UAs and SIP servers. Types of SIP servers include proxy, redirect, registrar, and presence. The part of a SIP UA that sends messages is known as the user agent client (UAC). The part of a SIP UA that receives messages is known as a user agent server (UAS).

SIP was originally designed for use over User Datagram Protocol (UDP). SIP servers, by default, listen on port 5060. Due to security concerns, SIP is now transitioning to Transmission Control Protocol (TCP) and transport layer security (TLS). SIP servers using TLS-over-TCP listen on port 5061. SIP UAs listen on a range of ports.

SIP uses the Session Description Protocol (SDP) to format the SIP message body in order to negotiate a Realtime Transport Protocol (RTP)/Realtime Transport Control Protocol (RTCP) connection between two or more UAs. The ports used for this will always be selected in a pair, with the even port used for RTP and the odd port for RTCP. SIP, because it uses SDP and RTP, causes many problems for standard firewalls. Neither SIP nor RTP are guaranteed to be symmetric, thus causing problems for stateful inspection firewalls that rely on symmetric flows. SIP and SDP carry IP addresses and ports embedded in the packet, and standard NAT implementations only modify the IP and TCP/UDP headers. A true SIP ALG is required to modify the packets as needed for NAT, but also to open holes in the firewall as needed for traffic flow based on the information carried in the SIP header.

Enabling the AOS SIP ALG (using the **ip firewall alg sip** command) configures the firewall to examine the ALL SIP packets it identifies and maintain knowledge of SIP transmissions on the network. Since SIP packet headers include port information for the call setup, the ALG must intelligently read the packets and remember the information.

ip firewall attack-log threshold *<number>*

Use the **ip firewall attack-log threshold** command to specify the number of possible attack conditions AOS will identify and block before generating a log message when using Internet Protocol version 4 (IPv4). Use the **no** form of this command to return to the default threshold.

> NOTE *The AOS IPv4 firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.*

Syntax Description

<number>	Specifies the number of possible attack conditions AOS IPv4 will identify before generating a log message. Valid range is **0** to **4294967295**.

Default Values

By default, the **ip firewall attack-log threshold** is set at **100**.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a threshold of **25** attacks before generating a log message for the IPv4 firewall:

(config)**#ip firewall attack-log threshold 25**

ip firewall check reflexive-traffic

Use the **ip firewall check reflexive-traffic** command to enable the AOS stateful inspection firewall to process Internet Protocol version 4 (IPv4) traffic from a primary subnet to a secondary subnet on the same interface through the firewall. Use the **no** form of this command to disable this feature.

The AOS IPv4 firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

No subcommands.

Default Values

All AOS IPv4 security features are disabled by default until the **ip firewall** command is issued at the Global Configuration mode prompt. In addition, the reflexive traffic check is disabled until the **ip firewall check reflexive-traffic** command is issued.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command allows the firewall to process IPv4 traffic from a primary subnet to a secondary subnet on the same interface through the firewall. If enabled, this IPv4 traffic will be processed through the access policy on that interface and any actions specified will be executed on the traffic.

Usage Examples

The following example enables the AOS IPv4 reflexive traffic check:

(config)**#ip firewall check reflexive-traffic**

ip firewall check rst-seq

Use the **ip firewall check rst-seq** command to enable Transmission Control Protocol (TCP) reset sequence number checking. Use the **no** form of this command to disable this feature.

The AOS firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

No subcommands.

Default Values

All AOS security features are disabled by default until the **ip firewall** command is issued at the Global Configuration mode prompt. In addition, TCP reset sequence number checking is disabled until the **ip firewall check rst-seq** command is issued.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example enables TCP reset sequence number checking:

(config)**#ip firewall check rst-seq**

ip firewall check syn-flood

Use the **ip firewall check syn-flood** command to enable the AOS stateful inspection firewall to filter out phony Transmission Control Protocol (TCP) service requests and allow only legitimate requests to pass through. Use the **no** form of this command to disable this feature.

> NOTE *The AOS firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.*

Syntax Description

No subcommands.

Default Values

All AOS security features are inactive until the **ip firewall** command is issued at the Global Configuration mode prompt. In addition, the SYN-flood check is enabled by default but remains inactive until the **ip firewall** command is issued.

Command History

Release 2.1	Command was introduced.

Functional Notes

SYN flooding is a well-known denial-of-service attack on TCP-based services. TCP requires a three-way handshake before actual communications begin between two hosts. A server must allocate resources to process new connection requests that are received. A potential intruder is capable of transmitting large amounts of service requests (in a very short period of time), causing servers to allocate all resources to process the phony incoming requests. Using the **ip firewall check syn-flood** command configures the AOS stateful inspection firewall to filter out phony service requests and allow only legitimate requests to pass through.

Usage Examples

The following example disables the AOS SYN-flood check:

(config)**#no ip firewall check syn-flood**

ip firewall check winnuke

Use the **ip firewall check winnuke** command to enable the AOS stateful inspection firewall to discard all out-of-band (OOB) data (to protect against WinNuke attacks). Use the **no** form of this command to disable this feature.

> NOTE *The AOS firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.*

Syntax Description

No subcommands.

Default Values

All AOS security features are inactive until the **ip firewall** command is issued at the Global Configuration mode prompt. In addition, WinNuke attack checking is disabled until the **ip firewall check winnuke** command is issued.

Command History

Release 2.1	Command was introduced.

Functional Notes

WinNuke attack is a well-known denial-of-service attack on hosts running Microsoft Windows® operating systems. An intruder sends OOB data over an established connection to a Windows user. Windows cannot properly handle the OOB data, and the host reacts unpredictably. Normal shut-down of the hosts will generally return all functionality. Using the **ip firewall check winnuke** command configures the AOS stateful inspection firewall to filter all OOB data to prevent network problems.

Usage Examples

The following example enables the firewall to filter all OOB data:

(config)**#ip firewall check winnuke**

ip firewall fast-allow-failover

Use the **ip firewall fast-allow-failover** command to automatically clear all open Internet Protocol version 4 (IPv4) firewall policy allow sessions when a route table change occurs. This allows the router to immediately send traffic to the failover interface. Otherwise, the router tries to send traffic from existing allowed policy sessions out from the failed IP address until the session times out, resulting in a loss of connectivity. This command should be configured when destination-specific rules are configured. Destination-specific rules are most often used in failover and IP load sharing configurations. Refer to the command *ip policy-class <ipv4 acp name> on page 1434* for more information. Use the **no** form of this command to disable this feature.

The AOS IPv4 firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

No subcommands.

Default Values

By default, all AOS IPv4 security features are disabled until the IPv4 firewall is enabled. By default, fast allow failover is disabled.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

In cases where failover takes place between an interface which uses network address translation (NAT) and an interface which does not use NAT, both **ip firewall fast-nat-failover** and **ip firewall fast-allow-failover** commands must be enabled. Using **fast-nat-failover** causes the policy session using NAT to be deleted when the session fails over and the route table changes to indicate a route that does not use NAT. Using **fast-allow-failover** causes the policy session to be deleted when the session is an allowed policy session and the route table changes to indicate a route that uses NAT.

Usage Examples

The following example enables **fast-allow-failover**:

(config)**#ip firewall fast-allow-failover**

ip firewall fast-nat-failover

Use the **ip firewall fast-nat-failover** command to automatically clear all open Internet Protocol version 4 (IPv4) firewall policy sessions when a route table change occurs. This allows the router to immediately send traffic to the failover interface. Otherwise, the router tries to send traffic from existing sessions out from the failed IP address until the session times out, resulting in a loss of connectivity. This command should be configured when destination-specific rules are configured. Destination-specific rules are most often used in failover and IP load sharing configurations. Refer to the command *ip policy-class <ipv4 acp name> on page 1434* for more information. Use the **no** form of this command to disable this feature.

The AOS IPv4 firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

No subcommands.

Default Values

By default, all AOS IPv4 security features are disabled until the IPv4 firewall is enabled. By default, fast NAT failover is disabled.

Command History

Release 9.3	Command was introduced.

Functional Notes

In cases where failover takes place between an interface which uses network address translation (NAT) and an interface which does not use NAT, both **ip firewall fast-nat-failover** and **ip firewall fast-allow-failover** commands must be enabled. Using **fast-nat-failover** causes the policy session using NAT to be deleted when the session fails over and the route table changes to indicate a route that does not use NAT. Using **fast-allow-failover** causes the policy session to be deleted when the session is an allowed policy session and the route table changes to indicate a route that uses NAT.

Usage Examples

The following example enables **fast-nat-failover**:

(config)**#ip firewall fast-nat-failover**

ip firewall fin-timeout <*value*>

Use the **ip firewall fin-timeout** command to specify the time period allowed for Transmission Control Protocol (TCP) FIN. Use the **no** form of this command to return to the default setting.

> *The AOS firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.*

Syntax Description

<*value*>	Specifies the time period in seconds allowed for TCP FIN. Range is **0** to **4294967295** seconds.

Default Values

By default, **ip firewall fin-timeout** is set to **4** seconds.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the TCP FIN time period to **120** seconds:

(config)**#ip firewall fin-timeout 120**

ip firewall local-traffic-only

Use the **ip firewall local-traffic-only** command to enable the Internet Protocol version 4 (IPv4) firewall for the processing of local traffic only. Forwarded traffic is not sent to the firewall when this feature is enabled. Use the **no** form of this command to disable the IPv4 firewall. Variations of this command include:

ip firewall local-traffic-only
ip firewall vrf <*name*> **local-traffic-only**

Syntax Description

vrf <*name*>	Optional. Specifies that the local traffic firewall is enabled on the specified virtual routing and forwarding (VRF) instance. If no VRF is specified, the firewall is enabled on the default (unnamed) VRF. Refer to *ip firewall vrf <name> on page 1390* for more information.

Default Values

By default, the IPv4 firewall is disabled.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

When the firewall is configured to process local traffic only (traffic arriving at the unit's local IP stack), routed traffic is allowed to flow through the AOS unit uninspected, but locally destined traffic is inspected by the firewall. This feature allows the firewall to protect local services running on the AOS unit even when routed traffic bypasses the firewall. When local traffic processing is enabled, several other security features are impacted, such as IPsec, policy classes, IP route cache, Generic Routing Encapsulation (GRE), and network address translation (NAT).

- Local traffic only firewall processing cannot be used with cryptography (**ip crypto**) because for IPsec to function, traffic must proceed through the firewall. If the firewall is configured to process local traffic only, routed traffic that requires IPsec protection will not flow through the firewall and therefore will not receive IPsec protection.
- Policy classes are applied only to traffic destined to the local stack when local traffic processing is enabled. The **self** policy class is applied to local traffic originating from the local stack, allowing all traffic, and cannot be changed.
- IP route cache entries are not created for local destinations or for the loopback interface when local traffic processing enabled.
- Local GRE traffic encapsulated by a GRE tunnel interface will bypass the firewall when local traffic processing is enabled.
- The full firewall is required any time NAT is needed to translate packets that would typically be forwarded by the AOS unit. The local firewall is not sufficient.

For additional IPv4 firewall configuration information, refer to *ip firewall on page 1367*.

Usage Examples

The following example enables the firewall for local traffic processing on the default VRF:

(config)**#ip firewall local-traffic-only**

ip firewall nat-preserve-source-port

Use the **ip firewall nat-preserve-source-port** command to enable the firewall to preserve the source port of a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) session for traffic going through source network address translation (NAT). By enabling this feature, the router will try to allocate NAT ports that match the original source ports of the traffic. If the source port is already allocated for a different traffic flow, it will choose the next available source port. Use the **no** form of this command to disable this feature. Variations of this command include the following:

ip firewall nat-preserve-source-port
ip firewall nat-preserve-source-port record-source-address

The AOS firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

record-source-address	Optional. Specifies that the original source port be preserved for multiple TCP/UDP traffic flows with the same source address.

Default Values

By default, the nat-preserve-source-port feature is enabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

Specifying **record-source-address** consumes 250 k of memory per public NAT IP address. Be sure there is adequate memory available before enabling this feature.

Usage Examples

The following example enables **nat-preserve-source-port**:

(config)**#ip firewall nat-preserve-source-port**

ip firewall policy-log threshold *<value>*

Use the **ip firewall policy-log threshold** command to specify the number of Internet Protocol version 4 (IPv4) access control policy (ACP) events identified by AOS before generating a log message. Use the **no** form of this command to return to the default value.

> NOTE *The AOS IPv4 firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.*

Syntax Description

<value>	Specifies the number of IPv4 policy events AOS identifies before creating the log. Valid range is **0** to **4294967295**.

Default Values

By default, the **ip firewall policy-log threshold** is set to **100**.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies that a log is generated when **150** IPv4 ACP events are detected on the default VRF:

(config)**#ip firewall policy-log threshold 150**

ip firewall rst-timeout <*value*>

Use the **ip firewall rst-timeout** command to specify the time period allowed for Transmission Control Protocol (TCP) reset. Use the **no** form of this command to return to the default setting.

The AOS firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

<*value*>	Specifies the time period in seconds allowed for TCP reset. Range is **0** to **4294967295** seconds.

Default Values

By default, **ip firewall rst-timeout** is set to **20** seconds.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the TCP reset time period to **120** seconds:

(config)**#ip firewall rst-timeout 120**

ip firewall stealth

Use the **ip firewall stealth** command to disable Internet Protocol version 4 (IPv4) Transmission Control Protocol (TCP) reset for denied IPv4 firewall associations. The stealth setting allows the route to be invisible as a route hop to associated devices. Use the **no** form of this command to disable this feature.

The AOS IPv4 firewall must be enabled (using the command ip firewall on page 1367) for the stateful inspection firewall to be activated.

Syntax Description

No subcommands.

Default Values

By default, the stealth option is disabled.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example enables the **stealth** option for the IPv4 firewall:

(config)**#ip firewall stealth**

ip firewall vrf *<name>*

Use the **ip firewall vrf** command to enable the firewall for a particular Internet Protocol version 4 (IPv4) virtual routing and forwarding (VRF) instance. The IPv4 firewall can be enabled or disabled independently for each VRF. Firewall settings are applied globally across all VRF instances and cannot be changed on an individual VRF basis. Refer to the command *ip firewall on page 1367* for more information on configuring IPv4 firewall settings. Use the **no** form of this command to disable the firewall for the specified VRF.

Syntax Description

<name>	Specifies the VRF instance.

Default Values

By default, the IPv4 firewall is disabled.

Command History

Release 17.1	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example enables the IPv4 firewall on the VRF named RED:

(config)**#ip firewall vrf RED**

ip flow cache sample one-out-of <*number*>

Use the **ip flow cache sample one-out-of** command to configure the integrated traffic monitoring (ITM) cache sampling rate. The **no** form of this command disables sampling. Variations of this command include:

ip flow cache sample one-out-of <*number*> **deterministic**
ip flow cache sample one-out-of <*number*> **random**

Syntax Description

deterministic	Specifies that traffic flow sampling be done at a fixed rate.
random	Specifies that traffic flow sampling be done at a random rate.
<*number*>	Specifies the number of traffic flow packets to be observed before another packet is sampled. Range is **1** to **255** packets.

Default Values

By default, sampling is disabled and every packet is recorded.

Command History

Release 16.1	Command was introduced.
Release 17.1	Command was expanded to include the **deterministic** keyword.

Functional Notes

Sampling provides a snapshot of traffic flow activity. It allows the cache to collect only one out of a specified number of IP packets that the interface is receiving or sending. Often, network traffic arrives in fixed patterns. This pattern can make statistics inaccurate if deterministic sampling is used. Therefore, random sampling is recommended over deterministic sampling to ensure an accurate sampling of traffic flow patterns. By reducing the amount of traffic flow data collected, sampling minimizes memory and CPU usage.

For users of large routers (for example, the NetVanta 5305), a sampling rate of greater than or equal to one out of every 100 packets is recommended.

Usage Examples

The following example configures ITM to sample one packet out of every **100** at a **random** sample rate:

(config)**#ip flow cache sample one-out-of 100 random**

ip flow cache timeout

Use the **ip flow cache timeout** command to configure the integrated traffic monitoring (ITM) cache for entry expiration. The **no** form of this command resets the expiration time to the default setting. Variations of this command include:

ip flow cache timeout active <*minutes*>
ip flow cache timeout inactive <*seconds*>

Syntax Description

active <*minutes*>	Specifies the amount of time a single traffic flow that continues to have packets detected at the observation point is stored before exportation. Range is **1** to **60** minutes.
inactive <*seconds*>	Specifies the amount of time that idle traffic flows (which no longer have packets detected at the observation point) are stored before exportation. Range is **10** to **600** seconds.

Default Values

By default, active flows are set to expire in **30** minutes, and inactive flows are set to expire in **15** seconds.

Command History

Release 16.1	Command was introduced.

Functional Notes

Traffic flow entry expiration can occur in one of three ways: (1) the configured expiration time has passed; (2) the Transmission Control Protocol (TCP) connection between the cache and the flow collector has expired due to FINISH/RESET signaling; or (3) critical configuration changes have been made (for example, changing the sampling rate). The default mode of expiration is based on a configured number of minutes for the traffic flow entry to be stored in the cache.

Usage Examples

The following example configures an expiration time of **15** minutes for **active** traffic flow entries:

(config)**#ip flow cache timeout active 15**

ip flow export

Use the **ip flow export** command to configure traffic flow data exportation parameters for integrated traffic monitoring (ITM). Use the **no** form of this command to disable the export functionality or to remove an associated destination if multiple entries are specified. Variations of this command include:

ip flow export destination <*ip address*> <*port*>
ip flow export destination <*ip address*> <*port*> **source** <*interface*>
ip flow export vrf <*name*> **destination** <*ip address*> <*port*>
ip flow export vrf <*name*> **destination** <*ip address*> <*port*> **source** <*interface*>

Syntax Description

destination <*ip address*> <*port*>	Specifies the IP address and User Datagram Protocol (UDP) port through which the destination will receive data export packets.
source <*interface*>	Specifies a source interface to send the data export packets. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Valid interfaces are those that can have an IP address. Type **source ?** for a complete list of valid interfaces.
vrf <*name*>	Specifies the virtual routing and forwarding (VRF) location to be used in data export.

Default Values

By default, **ip flow export** is disabled.

By default, if no source is specified, the router interface at the hop closest to the data collector will be sourced.

Command History

Release 16.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Up to two different destinations can be specified for traffic flow data export.

Using the source command specifies an interface from which to send the data export packets. If using a VRF destination, the source must be on the same VRF as the destination or it will be ignored and the routing table will determine the source interface. Most often, a source will only need to be specified for security purposes. For example, if an access control list (ACL) is active on the external data collector, a source interface may need to be specified.

Usage Examples

The following example configures the export destination to be the external data collector at the IP address **208.61.209.5** through the User Datagram Protocol (UDP) port **1010**.

(config)**#ip flow export destination 208.61.209.5 1010**

ip flow export template

Use the **ip flow export template** command to configure template exportation rates for integrated traffic monitoring (ITM). Use the **no** form of this command to return rate values to the default setting. Variations of this command include:

ip flow export template refresh-rate <*packets*>
ip flow export template timeout-rate <*minutes*>

Syntax Description

refresh-rate <*packets*>	Specifies the number of packets to be sent before the template information is sent to an external collector. Range is **1** to **600** packets.
timeout-rate <*minutes*>	Specifies the time in minutes that passes between instances of resending the template information. Range is **1** to **3600** minutes.

Default Values

By default, template information is sent every **20** packets, and template information is re-sent every **30** minutes.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example configures the template information to be sent every **50** packets:

(config)**#ip flow export template refresh-rate 50**

In the following example, traffic flow template information is configured to resend every **15** minutes:

(config)**#ip flow export template timeout-rate 15**

Technology Review

When exporting traffic flow data, there are multiple types of information sent to the external data flow collector. There is data information about each traffic flow, system information about each traffic flow, and the traffic flow record itself. The information about the traffic flow record is called a template. Templates are used to describe the types and lengths of individual header fields within a traffic flow data record. Templates also communicate to the external data collector what type of information to expect in the ITM flow record.

The following tables describe the information contained in each template.

Table 1. Data Template Information

Source IP Address
Destination IP Address
Transport Protocol Type
Source Port
Destination Port
Type of Service (ToS) Bits
Packets in a Flow
Bytes in a Flow
Interface (Input or Output)
System Up Time of First Packet
System Up Time of Last Packet
Flow Direction

Table 2. Options (System) Template Information

Active-Flow Timeout
Inactive-Flow Timeout
Sampling Rate
Sampling Algorithm (Random)
Total Packets Exported to Collectors
Total Flows Exported to Collectors
Total Bytes Exported to Collectors

Templates are sent to the external data collector after a user-specified number of expired traffic flow entries. They are also re-sent periodically at user-defined intervals. The templates must be re-sent periodically because User Datagram Protocol (UDP) is often unreliable, and the collector may discard all traffic flow data lacking valid template information.

ip flow top-talkers

Use the **ip flow top-talkers** command to enable Top Talker functionality for integrated traffic monitoring (ITM) and enter Top Talker configuration mode. Use the **no** form of this command to disable the Top Talkers functionality and remove all associated settings.

> NOTE *For Top Talkers functionality to be enabled, ITM must be enabled on an interface. Refer to the **ip flow egress | ingress** command. Refer to ip flow on page 2202 for more information on enabling ITM.*

Syntax Description

No subcommands.

Default Values

By default, the Top Talkers feature is disabled.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables top talkers:

```
(config)#ip flow top-talkers
(config-top-talkers)#
```

Technology Review

Using the internal Top Talkers data collection feature of ITM, several of the most important flow cache statistics can be viewed at a glance from within the router itself. The Top Talkers feature incorporates the statistics of Top Talkers (top bandwidth users by source IP address), Top Listeners (top bandwidth users by destination IP address), and Port Lists (amounts of traffic observed on specific ports) into easily viewed output, accessed through either the command line interface (CLI) or Web-based graphical user interface (GUI). These statistics are captured by the metering process at the traffic flow observation point, and collected as traffic flow entries expire from the flow cache. These statistics allow the user to see the nature of traffic being processed by the router without having to configure an external server to collect data.

The internal Top Talkers data collector can be enabled instead of or in conjunction with an external data collector, or it can operate with no external data collector configured. Because Top Talkers collects and processes expired flow cache entries in a separate function from their exportation, it can function independently of an external collector. With both an external data collector and Top Talkers enabled, expired flow cache entries are sent to both the external data collector and through the Top Talkers collector. The separation of Top Talkers collection from external data collectors provides methods of separate data collector configuration, therefore, allowing the enablement of only Top Talkers collection, Top Talkers collection in addition to external data collection, or external data collection only. For more information on the ITM Top Talkers feature, refer to the *Integrated Traffic Monitoring configuration guide* available online at https://supportcommunity.adtran.com.

ip forward-protocol udp <*value*>

Use the **ip forward-protocol udp** command to specify the protocols and ports AOS allows when forwarding broadcast packets. Use the **no** form of this command to disable a specified protocol or port from being forwarded. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the command to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the command to the default unnamed VRF. Specify a VRF instance other than the default by adding the **vrf** <*name*> parameter to the command as follows:

ip forward-protocol vrf <*name*> **udp** <*value*>

*The **ip forward-protocol udp** command can be used in conjunction with the **ip helper-address** command, issued in a valid interface, to configure AOS to forward User Datagram Protocol (UDP) broadcast packets.*

Syntax Description

<*value*>

Specifies the UDP traffic type (using source port).

The following is the list of UDP port numbers that may be identified using the text name:

biff (Port 512)
bootps (Port 67)
discard (Port 9)
dnsix (Port 195)
domain (Port 53)
echo (Port 7)
isakmp (Port 500)
mobileip (Port 434)
nameserver (Port 42)
netbios-dgm (Port 138)
netbios-ns (Port 137)
netbios-ss (Port 139)
ntp (Port 123)
pim-auto-rp (Port 496)
rip (Port 520)
snmp (Port 161)
snmptrap (Port 162)
sunrpc (Port 111)
syslog (Port 514)
tacacs (Port 49)
talk (Port 517)
tftp (Port 69)
time (Port 37)
who (Port 513)
xdmcp (Port 177)

Alternately, the <*value*> may be specified using the following syntax: <0-65535>. Specifies the port number used by UDP to pass information to upper layers. All ports below 1024 are considered well-known ports and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above 1024 are dynamically assigned ports that include registered ports for vendor-specific applications.

vrf <*name*>

Specifies the name of the VRF on which to configure broadcast packet forwarding other than the default VRF instance.

Default Values

By default, AOS forwards broadcast packets for all protocols and ports.

Command History

Release 2.1	Command was introduced.

Functional Notes

Use this command to configure AOS to forward UDP packets across the wide area network (WAN) link to allow remote devices to connect to a UDP service on the other side of the WAN link.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface eth 0/1**
(config-eth 0/1)**#ip helper-address 192.33.5.99**

ip ftp access-class <*acl*> in

Use the **ip ftp access-class in** command to assign an access control list (ACL) to all self-bound File Transfer Protocol (FTP) incoming sessions. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ftp access-class <*acl*> **in**
ip ftp access-class <*acl*> **in any-vrf**
ip ftp access-class <*acl*> **in vrf** <*name*>

Syntax Description

<*acl*>	Specifies the ACL to apply to the FTP traffic.
in	Specifies that the ACL is applied to incoming FTP connections.
any-vrf	Optional. Allows incoming FTP connections from any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Allows incoming FTP connections from a specified VRF instance.

Default Values

By default, all FTP access is allowed.

Command History

Release 2.1	Command was introduced.
Release R10.7.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example applies the configured ACL, named **Inbound_FTP**, to inbound FTP traffic:

(config)**#ip ftp access-class Inbound_FTP in**

ip ftp server

Use the **ip ftp server** command to enable the File Transfer Protocol (FTP) server and optionally specify the default location for the FTP server to store and retrieve files. Use the **no** form of this command to disable the FTP server. Variations of this command include:

ip ftp server
ip ftp server default-filesystem cflash
ip ftp server default-filesystem flash
ip ftp server default-filesystem ramdisk
ip ftp server default-filesystem usbdrive0

Syntax Description

default-filesystem	Specifies the default file system for the FTP server to use.
cflash	Optional. Specifies the FTP server use the CompactFlash® card as the default file system.
flash	Optional. Specifies that the FTP server use the system flash as the default file system.
ramdisk	Optional. Specifies that the FTP server use the volatile RAM disk as the default file system.
usbdrive0	Optional. Specifies that the FTP server use the Universal Serial Bus (USB) flash drive as the default file system.

Default Values

By default, the **ip ftp server default-filesystem** is set to **flash**.

Command History

Release 13.1	Command was introduced.
Release 17.7	Command was expanded to include the **ramdisk** parameter.
Release 18.2	Command was expanded to include the **usbdrive0** parameter.

Usage Examples

The following example enables the FTP server:

(config)**#ip ftp server**

The following example specifies **cflash** file system as the default:

(config)**#ip ftp server default-filesystem cflash**

ip ftp source-interface <*interface*>

Use the **ip ftp source-interface** command to use the specified interface's IP address as the source IP address for File Transfer Protocol (FTP) traffic transmitted by the unit. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the configuration to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the configuration to the default unnamed VRF. Use the **no** form of this command if you do not wish to override the default source IP address. Variations of this command include:

ip ftp source-interface <*interface*>
ip ftp vrf <*name*> **source-interface** <*interface*>

Syntax Description

<*interface*>	Specifies the interface to be used as the source IP address for FTP traffic. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip ftp source-interface ?** for a complete list of valid interfaces.
vrf <*name*>	Specifies the name of the VRF to which to configure the source interface.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 9.1	Command was expanded to include the high level data link control (HDLC) interface.
Release 14.1	Command was expanded to include the tunnel interface.
Release 15.1	Command was expanded to include the bridged virtual interface (BVI).
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for FTP traffic:

(config)**#ip ftp source-interface loopback 1**

The following example configures the unit to use the **loopback 1** interface as the source IP for FTP traffic on the VRF RED:

(config)**#ip ftp vrf RED source-interface loopback 1**

ip hw-access-list extended <*name*>

Use the **ip hw-access-list extended** command to create and name an IP hardware access control list (ACL). This command also enters the ACL's configuration mode. Using the **no** form of this command deletes the IP hardware ACL.

For a complete list of all IP hardware ACL configuration commands, refer to the *Hardware ACL and Access Map Command Set on page 4235*.

Syntax Description

<name>	Specifies the name of the IP hardware ACL.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware ACLs.

Command History

Release 17.6	Command was introduced.

Functional Notes

This command only creates an empty hardware ACL, it does not configure it. For additional IP hardware ACL configuration commands and configuration parameters, refer to the *Hardware ACL and Access Map Command Set on page 4235* or the *Hardware ACLs in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates an IP hardware ACL **Trusted** and enters the IP hardware ACL configuration mode:

```
(config)#ip hw-access-list extended Trusted
        Configuring New IP Hardware Extended ACL "Trusted"
(config-ext-ip-hw-nacl)#
```

Technology Review

Hardware ACLs are used as traffic selectors by the hardware access maps; by themselves they do nothing. Hardware ACLs are composed of an ordered list of entries with an implicit **deny any** at the end of each list. A hardware ACL with no entries includes an implicit **permit any**. An ACL entry contains two parts: an action (**permit** or **deny**) and a frame pattern. A **permit** ACL matches frames (meeting the specified pattern) and allows them to enter the router system. A **deny** ACL advances AOS to the next access list entry.

ACL criteria are compared to the incoming frame in the order in which they were entered or from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

ip igmp join <*ip address*>

Use the **ip igmp join** command to instruct the router stack to join a specific group. The stack may join multiple groups. Use the **no** form of this command to disable this feature.

Syntax Description

<*ip address*>	Specifies the IP address of a multicast group. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command aids in debugging, allowing the router's IP stack to connect to and respond on a multicast group. The local stack operates as an Internet Control Messaging Protocol (ICMP) host on the attached segment. In multicast stub applications, the global helper address takes care of forwarding IGMP joins/responses on the upstream interface. The router may respond to ICMP echo requests for the joined groups.

Usage Examples

The following example configures the unit to join with the specified multicast group:

(config)**#ip igmp join 172.0.1.50**

ip igmp snooping

Use the **ip igmp snooping** command to globally enable Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable global IGMP snooping.

Syntax Description

No subcommands.

Default Values

By default, IGMP snooping is disabled.

Command History

Release 12.1	Command was introduced.
Release R10.10.0	Command was removed from the 1234 (2nd Generation), 1234P (2nd Generation), 1238 (2nd Generation), 1238P (2nd Generation), 1534 (2nd Generation), 1534P (2nd Generation), 1535, 1535P, 1544 (2nd Generation), 1544P (2nd Generation), 1638, and 1638P.

Functional Notes

IGMP snooping is a method of preventing switches from flooding all ports with received multicast streams. By monitoring the conversations between a host and a router, the switch can determine which multicast streams will interest a host and load its own forwarding tables to take advantage of that knowledge. When the host sends a leave message to the router, the switch removes the entries after a timeout period.

On the 1534 (1st Generation), 1234 (1st Generation), 1238 (1st Generation), and 1335 platforms, global IGMP snooping must be enabled in order to enable virtual local area network (VLAN) IGMP snooping.

Usage Examples

The following example globally enables IGMP snooping:

(config)**#ip igmp snooping**

ip igmp snooping flood-unknown

Use the **ip igmp flood-unkown** to enable flooding of VLAN ports for unknown multicast frames. Use the **no** form of this command to disable global IGMP snooping.

Syntax Description

No subcommands.

Default Values

By default, flooding of unkown multicast frames is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example globally enables IGMP snooping:

(config)**#ip igmp snooping**

ip igmp snooping immediate-leave vlan <*vlan id*>

Use the **ip igmp snooping immediate-leave vlan** command to enable the immediate leave setting of Internet Group Management Protocol (IGMP) snooping on the specified virtual local area network (VLAN). With immediate leave enabled, the AOS device immediately removes a port from the IP multicasting group after detecting an IGMP leave message on that port. To enable the immediate leave setting, you must first enable IGMP snooping on the VLAN using the command *ip igmp snooping on page 1407*. Use the **no** form of this command to disable VLAN IGMP snooping.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Range is **1** to **4095**.

Default Values

By default, VLAN IGMP immediate leave is disabled.

Command History

Release R 11.5.0	Command was introduced.

Functional Notes

When a host sends a leave group message, a multicast router sends a group-specific query to determine if any other hosts respond on that port. If no response is received and the query times out, the AOS device removes the port from the IP multicasting group. The immediate leave setting, allows the AOS device to remove the port without waiting for the query to time out.

Usage Examples

The following example enables IGMP immediate leave on VLAN 1:

(config)**#ip igmp snooping immediate-leave vlan 1**

ip igmp snooping querier vlan *<vlan id> <source address>*

Use the **ip igmp snooping querier vlan** command to enable the Internet Group Management Protocol (IGMP) snooping querier on the specified VLAN . Use the **no** form of this command to disable this feature.

Syntax Description

<vlan id>	Specifies a valid VLAN interface ID on which the querier will be enabled. Range is **1** to **4094**.
<source address>	Specifies the source address used for IGMP query packets.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Functional Notes

IGMP snooping requires the presence of an IGMP querier in order to function properly. This roll is normally played by a multicast router on the local network. However, in cases where a Layer 3 switch is deployed, the switch itself may be the unicast router and a multicast router may not be present. When no multicast router exists in the VLAN to originate the queries, an IGMP snooping querier must be configured to send membership queries. When enabled, the IGMP querier will send general IGMPv2 queries every 125 seconds.

Usage Examples

The following example enables the IGMP snooping querier on VLAN ID **1** with a source address of **10.10.10.1**:

(config)**#ip igmp snooping querier vlan 1 10.10.10.1**

ip igmp snooping querier period <*seconds*>

Use the **ip igmp snooping querier period** command to set the interval at which the Internet Group Management Protocol (IGMP) snooping querier will send out IGMPv2 snooping queries. Use the **no** form of this command to disable this feature.

Syntax Description

<*seconds*>	Specifies the number of seconds between sent queries. Range is **10** to **1000** seconds.

Default Values

By default, the querier period is **125** seconds.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

IGMP snooping requires the presence of an IGMP querier in order to function. This roll is normally played by a multicast router on the local network. However, in cases where a Layer 3 switch is deployed, the switch itself may be the unicast router and a multicast router may not be present. When no multicast router exists in the VLAN to originate the queries, an IGMP snooping querier must be configured to send membership queries. When enabled, the IGMP querier will send general IGMPv2 queries every 125 seconds.

Usage Examples

The following example specifies a **10** seconds IGMP snooping querier period:

(config)**#ip igmp snooping querier period 10**

ip igmp snooping vlan *<vlan id>*

Use the **ip igmp snooping vlan** command to enable Internet Group Management Protocol (IGMP) snooping on the specified virtual local area network (VLAN). Use the **no** form of this command to disable VLAN IGMP snooping.

Syntax Description

<vlan id>	Specifies a valid VLAN interface ID. Range is **1** to **4095**.

Default Values

By default, VLAN IGMP snooping is disabled on all platforms. However, enabling global IGMP snooping on the 1534 (1st Generation), 1234 (1st Generation), 1238 (1st Generation), and 1335 platformsalso enables VLAN IGMP snooping.

Command History

Release 12.1	Command was introduced.

Functional Notes

IGMP snooping is a method of preventing switches from flooding all ports with received multicast streams. By monitoring the conversations between a host and a router, the switch can determine which multicast streams will interest a host and load its own forwarding tables to take advantage of that knowledge. When the host sends a leave message to the router, the switch removes the entries after a timeout period.

On the 1534 (1st Generation), 1234 (1st Generation), 1238 (1st Generation), and 1335 platforms, global IGMP snooping must be enabled in order to enable virtual local area network (VLAN) IGMP snooping.

Usage Examples

The following example enables IGMP snooping on VLAN 1:

(config)**#ip igmp snooping vlan 1**

ip igmp snooping vlan <*vlan id*> mrouter interface <*interface*>

Use the **ip igmp snooping vlan mrouter interface** command to add a static connection to a multicast router. Use the **no** form of this command to remove a static connection to a multicast router.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Range is **1** to **4094**.
<*interface*>	Specifies an interface to be added to the multicast router. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip igmp snooping vlan** <*vlan id*> **mrouter interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example adds Ethernet interface 0/1 to the list of multicast router interfaces:

(config)**#ip igmp snooping vlan 1 mrouter interface ethernet 0/1**

ip igmp snooping vlan <*vlan id*> static <*mac address*> interface <*interface*>

Use the **ip igmp snooping vlan static interface** command to statically configure a Layer 2 interface as a member of a multicast group. Use the **no** form of this command to remove a Layer 2 interface from a multicast group.

Syntax Description

<*vlan id*>	Specifies the VLAN ID of the multicast group. Range is **1** to **4094**.
<*mac address*>	Specifies the group's 48-bit medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
<*interface*>	Specifies an interface identification for the member interface. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip igmp snooping vlan** <*vlan id*> **static** <*mac address*> **interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Functional Notes

There are two types of multicast addresses: MAC addresses and IP addresses. A multicast IP address is a Class D address (**224.0.0.0** to **239.255.255.255**). These addresses are also referred to as group destination addresses (GDAs). Each GDA has an associated multicast MAC address. A multicast MAC address is formed by using the prefix 01-00-5e followed by the last 23 bits of the GDA. The <*mac address*> specified in this command must be a multicast MAC address. The following table shows examples of multicast MAC addresses.

Multicast Addresses

Multicast IP Address	Multicast MAC Address
226.10.10.10	01-00-5e-0a-0a-0a
228.20.20.20	01-00-5e-14-14-14
230.30.30.30	01-00-5e-1e-1e-1e

This mapping of IP addresses is a many-to-one relationship. For example, 226.10.10.10 maps to the same MAC address as 227.10.10.10. The entire Class D network is not available for multicast. The following table shows the reserved addresses.

Reserved Multicast IP Addresses

224.0.0.1	All Multicast-capable hosts
224.0.0.2	All Multicast-capable routers
224.0.0.5 and 224.0.0.6	Reserved for OSPF
224.0.0.1 to 224.0.0.255	Generally reserved for various protocols

Usage Examples

The following example configures the Ethernet interface 0/1 as a member of the multicast group with multicast MAC address **01:00:5E:01:01:01**:

(config)**#ip igmp snooping vlan 1 static 01:00:5E:01:01:01 interface ethernet 0/1**

ip load-sharing

Use the **ip load-sharing** command to configure whether parallel routes in the route table are used to load-share forwarded packets. If this command is disabled, the route table uses a single “best” route for a given subnet. If this command is enabled, the route table can use multiple “best” routes and alternate between them. Use the **no** form of this command to disable this feature. Variations of this command include:

ip load-sharing per-destination
ip load-sharing per-packet

Syntax Description

per-destination	Specifies that the route used for forwarding a packet be based on a hash of the source and destination IP address in the packet.
per-packet	Specifies that each forwarding route lookup rotates through all the parallel “best” routes. (Parallel routes are defined as routes to the same subnet with the same metrics that only differ by their next-hop address.)

Default Values

By default, ip load-sharing is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example turns on load-sharing per destination:

(config)**#ip load-sharing per-destination**

The following example disables load-sharing:

(config)**#no ip load-sharing**

ip local policy route-map <*name*>

Use the **ip local policy route-map** command to specify a route map for local policy routing on the device. This setting is applied to the local network interface. It can be further specified to a specific virtual routing and forwarding (VRF) by adding the VRF name. Use the **no** form of this command to return to the default route map. Variations of this command include:

ip local policy route-map <*name*>
ip local policy route-map <*name*> **vrf** <*name*>

Syntax Description

<*name*>	Specify the name of the route map.
vrf <*name*>	Optional. Specifies a nondefault VRF on which to define the local policy route map.

Default Values

By default, this command is disabled.

Command History

Release 11.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

Before a route map can be specified, it must first be defined using the route-map command. Refer to *route-map on page 1687* for more information.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

There is only one local policy for each VRF instance.

Usage Examples

The following example specifies a route map entitled **myMap** for local policy routing:

(config)**#ip local policy route-map myMap**

ip mcast-stub helper-address *<ip address>*

Use the **ip mcast-stub helper-address** command to specify an IP address toward which Internet Group Management Protocol (IGMP) host reports and leave messages are forwarded. This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub downstream** and **ip mcast-stub upstream** commands. Use the **no** form of this command to return to the default setting.

Syntax Description

<ip address>	Specifies the address to which the IGMP host reports and leave messages are forwarded. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no helper-address is configured.

Command History

Release 7.1	Command was introduced.

Functional Notes

The helper address is configured globally and applies to all multicast-stub downstream interfaces. The address specified may be the next upstream hop or any upstream address on the distribution tree for the multicast source, up to and including the multicast source. The router selects, from the list of multicast-stub upstream interfaces, the interface on the shortest path to the specified address. The router then proxies, on the selected upstream interface (using an IGMP host function), any host joins/leaves received on the downstream interface(s). The router retransmits these reports with addresses set as if the report originated from the selected upstream interface.

For example, if the router receives multiple joins for a group, it will not send any extra joins out the upstream interface. Also, if it receives a leave, it will not send a leave until it is certain that there are no more subscribers on any downstream interface.

Usage Examples

The following example specifies 172.45.6.99 as the helper address:

(config)**#ip mcast-stub helper-address 172.45.6.99**

ip mgcp

Use the **ip mgcp** command to enable the Media Gateway Control Protocol (MGCP) stack. Use the **no** form of this command to disable the MGCP stack.

Syntax Description

No subcommands.

Default Values

By default, the MGCP stack is disabled.

Command History

Release A2	Command was introduced.

Usage Examples

The following example enables the MGCP stack:

(config)**#ip mgcp**

ip mgcp bracketed-ip

Use the **ip mgcp bracketed-ip** command to prevent bracketed IP address format from being used in specifying Media Gateway Control Protocol (MGCP) endpoint names. Use the **no** form of this command to disable the bracket requirement when entering MGCP endpoint IP addresses.

Syntax Description

No subcommands.

Default Values

By default, brackets are used when specifying MGCP endpoints.

Command History

Release A2	Command was introduced.

Functional Notes

Some call agents require that brackets be used when an MGCP gateway uses an IP address as its local domain name, and some call agents do not support the bracketed format. Bracketed IP addresses are displayed as **endpointname@[xx.xx.xx.xx]**, whereas nonbracketed endpoint IP addresses are displayed as **endpointname@xx.xx.xx.xx**. Using this command allows the user to control whether IP addresses will be bracketed or not, rather than entering all IP addresses as bracketed IP addresses.

Usage Examples

The following example disables bracketed IP address control:

(config)**#no ip mgcp bracketed-ip**

ip mgcp call-agent primary *<hostname | ipv4 address>*

Use the **ip mgcp call-agent primary** command to specify the primary Media Gateway Control Protocol (MGCP) call agent host name. Use the **no** form of this command to remove the specified primary call agent.

Syntax Description

<hostname | ipv4 address>	Specifies the call agent host name. Host names can be entered as either a fully qualified domain name (FQDN) or as an IP version 4 (IPv4) address in dotted decimal notation (**XX.XX.XX.XX**).

Default Values

By default, no primary call agents are configured.

Command History

Release A2	Command was introduced.

Functional Notes

The **ip mgcp call-agent primary** command identifies the call agent to the media gateway. Both primary and secondary call agents can be established, but at minimum a primary call agent is required. If a connection with the primary call agent fails, call agents will be tried in the order they are entered in the configuration. For more information regarding call agents and MGCP configuration, refer to the *MGCP in AOS* configuration guide available online at https://supportcommunity.adtran.com.

NOTE *The **no** form of this command will only take effect if there are no secondary call agents configured. If secondary call agents are configured, the primary call agent can be modified by issuing this command with the new host name information.*

NOTE *The primary call agent host name cannot be removed while any secondary call agents are configured. For more information about secondary call agents, refer to the command* *ip mgcp call-agent secondary <hostname | ipv4 address> on page 1422*.

Usage Examples

The following example configures the primary MGCP call agent, **ca1.company.com**:

(config)**#ip mgcp call-agent primary ca1.company.com**

ip mgcp call-agent secondary *<hostname | ipv4 address>*

Use the **ip mgcp call-agent secondary** command to specify the secondary Media Gateway Control Protocol (MGCP) call agent host name. Use the **no** form of this command to remove the specified secondary call agent.

Syntax Description

<hostname | ipv4 address>	Specifies the call agent host name. Host names can be entered as either a fully qualified domain name (FQDN) or as an IP version 4 (IPv4) address in dotted decimal notation (**XX.XX.XX.XX**).

Default Values

By default, no secondary call agents are configured.

Command History

Release A2	Command was introduced.

Functional Notes

Multiple secondary call agent host names can be configured. If a connection with the primary call agent fails, call agents are tried in the order they are entered in the configuration. New secondary call agents are added at the end of the list.

If secondary call agents are configured, primary call agents cannot be removed. For more information about primary call agents, refer to the command *ip mgcp call-agent primary <hostname | ipv4 address> on page 1421*.

Usage Examples

The following example specifies the secondary MGCP call agent as **ca2.company.com**:

(config)**#ip mgcp call-agent secondary ca2.company.com**

ip mgcp local-domain-name

Use the **ip mgcp local-domain-name** command to specify the local Media Gateway Control Protocol (MGCP) domain name. Use the **no** form of this command to remove the associated host name from the AOS product. Variations of this command include:

ip mgcp local-domain-name <*hostname* | *ipv4 address*>
ip mgcp local-domain-name media-gateway

Syntax Description

<*hostname*	*ipv4 address*>	Specifies the gateway host name in either a fully qualified domain name (FQDN) format or as an IP version 4 (IPv4) address in dotted decimal notation (**XX.XX.XX.XX**).
media-gateway	Specifies that the local domain name is based on the media gateway setting on the physical interface used for outbound traffic (for example, the Point-to-Point Protocol (PPP) or the Ethernet interfaces).

Default Values

By default, a local domain name is not configured.

Command History

Release A2	Command was introduced.

Usage Examples

The following example specifies that the local domain name for the media gateway is **mygateway@company.com**:

(config)#**ip mgcp local-domain-name mygateway@company.com**
(config)#

ip mgcp max1 <*value*>

Use the **ip mgcp max1** command to specify the number of Media Gateway Control Protocol (MGCP) message retransmissions between the gateway and the call agent. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the number of message retransmissions that will occur between the gateway and the call agent while the gateway waits for a response from the call agent. Range is **1** to **255**.

Default Values

By default, the **max1** value is set to **5**.

Command History

Release A2	Command was introduced.

Functional Notes

If the gateway does not receive a response from the call agent, the gateway retransmits MGCP messages **max1** times before the gateway either queries the domain naming system (DNS) to detect a possible change in call agent interfaces or directs transmissions to alternate call agent IP addresses.

For more information about MGCP configuration, refer to the *MGCP in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example sets the number of message transmissions between the gateway and the call agent to **20**:

(config)**#ip mgcp max1 20**

ip mgcp max2 <*value*>

Use the **ip mgcp max2** command to specify the number of Media Gateway Control Protocol (MGCP) message retransmissions between the MGCP gateway and the call agent before the gateway disconnects. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the number of message retransmissions that will occur before the gateway disconnects from the call agent. Range is **1** to **255**.

Default Values

By default, MGCP retransmissions before gateway disconnection is set to **7**.

Command History

Release A2	Command was introduced.

Functional Notes

When the gateway has retransmitted MGCP messages **max2** times, it indicates that the gateway has already exceeded the **max1** value (refer to the command *ip mgcp max1 <value> on page 1424*) and it will contact the domain naming system (DNS) to search for alternate call agent interfaces which to connect. If the gateway does not find any available call agent interfaces for connection, the gateway will disconnect.

*The **max2** value must always be greater than the **max1** value. If the **max1** value is specified to be greater than the **max2** value, the **max2** value is automatically defined as **max1** + **1**.*

For more information about MGCP configuration, refer to the *MGCP in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the MGCP gateway will retransmit MGCP messages **30** times before disconnecting from the call agent:

(config)**#ip mgcp max2 30**

ip mgcp persistent-notify

Use the **ip mgcp persistent-notify** command to enable persistent event notification to the Media Gateway Control Protocol (MGCP) call agent. Use the **no** form of this command to disable persistent notification. Variations of this command include:

ip mgcp persistent-notify hd
ip mgcp persistent-notify hu
ip mgcp persistent-notify hf

*Multiple combinations of the **hd**, **hu**, and **hf** parameters can be entered.*

Enabling persistent notification when it is not required can cause unexpected and undesired operation.

Syntax Description

hd	Specifies that notification of endpoint hang down is sent to the call agent.
hu	Specifies that notification of endpoint hang up is sent to the call agent.
hf	Specifies that notification of endpoint hook flash is sent to the call agent.

Default Values

By default, persistent notification is disabled.

Command History

Release A2	Command was introduced.

Functional Notes

When persistent notification is disabled, the media gateway will not send event notifications of endpoint hang down (**hd**), hang up (**hu**), or hook flash (**hf**). When the feature is enabled, the media gateway will send notification of endpoint events even if it has not received a notification request from the call agent. Some call agents require the use of persistent notification. For example, sometimes hd notification is required for initial dial tone once the link has become active. Refer to the configuration materials provided with your call agent for more information.

Usage Examples

The following example enables persistent notification of endpoint hang down:

(config)**#ip mgcp persistent-notify hd**

ip mgcp qos dscp <*value*>

Use the **ip mgcp qos dscp** command to specify the differentiated services code point (DSCP) value in the Media Gateway Control Protocol (MGCP) packets transmitted by the MGCP gateway. This value can be used by quality of service (QoS) mechanisms to give priority for this type of traffic. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the DSCP value. Range is **0** to **63**.

Default Values

By default, the DSCP value for MGCP packets is **46**.

Command History

Release A2	Command was introduced.

Usage Examples

The following example specifies the DSCP value for MGCP gateways as **10**:

(config)**#ip mgcp qos dscp 10**

ip mgcp retransmit-delay

Use the **ip mgcp retransmit-delay** command to specify the constant time between retransmissions of Media Gateway Control Protocol (MGCP) messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip mgcp retransmit-delay 100ms
ip mgcp retransmit-delay 250ms
ip mgcp retransmit-delay 500ms
ip mgcp retransmit-delay 1sec
ip mgcp retransmit-delay 2sec
ip mgcp retransmit-delay 4sec

Syntax Description

100ms	Specifies 100 milliseconds between retransmissions.
250ms	Specifies 250 milliseconds between retransmissions.
500ms	Specifies 500 milliseconds between retransmissions.
1sec	Specifies 1 second between retransmissions.
2sec	Specifies 2 seconds between retransmissions.
4sec	Specifies 4 seconds between retransmissions.

Default Values

By default, retransmissions occur with longer and longer delays between retransmissions. These delays are based on RFC 3435, which uses a User Datagram Protocol (UDP) back-off algorithm for MGCP retransmission delay.

Command History

Release A2	Command was introduced.

Usage Examples

The following example specifies that retransmissions will occur at a constant rate of **1sec**:

(config)**#ip mgcp retransmit-delay 1sec**

ip mgcp rfc2833-signaling

Use the **ip mgcp rfc2833-signaling** command to enable the transmission and reception of ABCD signal bits via RFC 2833 packets. Use the **no** form of this command to disable ABCD signaling.

This command should only be used with gateways configured to send ABCD signaling bits out-of-band for TDM passthrough. Configuring this command when it is not needed will likely cause undesired operation.

Syntax Description

No subcommands.

Default Values

By default, ABCD signaling is disabled.

Command History

Release A2	Command was introduced.

Usage Examples

The following example enables ABCD signaling:

(config)**#ip mgcp rfc2833-signaling**

ip mgcp standard

Use the **ip mgcp standard** command to specify the Media Gateway Control Protocol (MGCP) standard the gateway will use. Use the **no** form of this command to return to the default standard. Variations of this command include:

ip mgcp standard rfc3435
ip mgcp standard ncs

Syntax Description

rfc3435	Specifies that the RFC 3435 MGCP standard is used.
ncs	Specifies that the MGCP 0.1/NCS 1.0 standard is used.

Default Values

By default, MGCP gateways use the **rfc3435** standard.

Command History

Release A2	Command was introduced.

Usage Examples

The following example sets the MGCP standard to **ncs**:

(config)**#ip mgcp standard ncs**

ip mgcp udp <*port*>

Use the **ip mgcp udp** command to specify the local listening port for the Media Gateway Control Protocol (MGCP) stack for User Datagram Protocol (UDP) information. Use the **no** form of this command to return to the default port.

Syntax Description

<*port*>	Specifies the port to listen for UDP information. Range is **1** to **65535**.

Default Values

By default, the MGCP gateway listens for UDP on port **2427** as defined by RFC 3435.

Command History

Release A2	Command was introduced.

Usage Examples

The following example specifies that the MGCP gateway will listen for UDP information on port **2727**:

(config)**#ip mgcp udp 2727**

ip multicast-routing

Use the **ip multicast-routing** command to enable the multicast router process. The command does not affect other multicast-related configurations. Use the **no** form of this command to disable this feature. Disabling this command prevents multicast forwarding, but does not remove other multicast commands and processes.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables multicast functionality:

(config)**#ip multicast-routing**

ip nat pool *<name>*

Use the **ip nat pool** command to create a new static 1:1 network address translation (NAT) pool and enter its configuration command set. This command can also be used to enter the command set for an existing pool. Use the **no** form of this command to remove a configured NAT pool. Refer to the command *load-protect on page 1575* for more information about mapping addresses for static 1:1 NAT pools. Variations of this command include:

ip nat pool *<name>*
ip nat pool *<name>* **static**

Syntax Description

<name>	Enters the configuration commands set for an existing NAT pool identified by the *<name>* variable.
<name> **static**	Creates NAT pool for 1:1 static NAT and enters its configuration command set. For a given configuration, a local address statically maps to a global address and vice versa.

Default Values

By default, there are no NAT pools configured.

Command History

Release 17.4	Command was introduced to allow static NAT pools only.

Functional Notes

Static 1:1 NAT allows connections initiated from a particular private IP address to always map to a particular public IP address. For every private host that requires a 1:1 NAT mapping, there must be a corresponding NAT address on the public side. In previous versions of AOS, this was accomplished by using an exhaustive list of all address mappings. AOS version 17.4 and later provided support for using NAT pools that lists ranges of local and global IP addresses to create the 1:1 mappings.

Usage Examples

The following example creates a static 1:1 NAT pool named **POOL1** and enters the NAT pool configuration command set:

(config)**#ip nat pool POOL1 static**

The following example enters the configuration command set for an existing NAT pool named **POOL2**:

(config)**#ip nat pool POOL2**

ip policy-class *<ipv4 acp name>*

Use the **ip policy-class** command to create an Internet Protocol version 4 (IPv4) access control policy (ACP) and enter the IPv4 ACP command set. Use the **no** form of this command to delete an IPv4 ACP and all the entries it contains. Refer to the *IPv4 Access Control Policy Command Set on page 4278*.

Configured IPv4 ACPs will only be active if the command ip firewall on page 1367 has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.

Before applying an ACP to an interface, verify your Telnet or secure shell (SSH) connection will not be affected by the policy. If an ACP is applied to the interface you are connecting through and it does not allow Telnet or SSH traffic, your connection will be lost.

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP using an alphanumeric descriptor (maximum of 50 characters). All ACP descriptors are case sensitive.

Default Values

By default, all AOS IPv4 security features are disabled and there are no configured ACP entries.

Command History

Release 2.1	Command was introduced.

Functional Notes

AOS IPv4 ACPs are used to allow, discard, or manipulate (using network address translation (NAT)) data for each physical interface. Each ACP consists of an action (**allow**, **discard**, **nat**) and a selector access control list (ACL). When IPv4 packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

*An implicit discard exists at the end of every IPv4 ACP. Specifying a **discard list** is unnecessary in most applications and should be used with caution. A **discard list** can adversely affect certain functions of a unit (virtual private network (VPN), routing protocols, etc.). Specifying an empty ACL or a nonexistent ACL in an ACP will result in an implicit permit.*

IPv4 ACPs and ACLs cannot have the same name as a configured IPv6 ACP or ACL.

Usage Examples

The following example creates an IPv4 ACP named **PRIVATEv4**:

(config)**#ip policy-class PRIVATEv4**
(config-policy-class)#

Technology Review

IPv4 ACPs and ACLs regulate traffic through the routed network. Creating IPv4 ACPs and ACLs to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the IPv4 security features of AOS using the **ip firewall** command. Refer to the command *ip firewall on page 1367* for more information.

Step 2:
Create an IPv4 ACP that uses a configured ACL by issuing the **ip policy-class** command. AOS IPv4 ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each ACP consists of an action (**allow**, **discard**, **nat**) and a selector (ACL). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded.

Step 3:
Create an IPv4 ACL to permit or deny specified traffic by using either the **ip access-list extended** or **ip access-list standard** command. Standard IPv4 ACLs match based on the source IP address of the packet. Extended IPv4 ACLs match based on the source and destination of the packet. Refer to the command *ip access-list extended <ipv4 acl name> on page 1344* or the command *ip access-list standard <ipv4 acl name> on page 1346* for more information. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IP address.

2. Using host <*ip address*> to specify a single host address.

3. Using the <*ip address*> <*wildcard*> format to match all IPv4 addresses in a range. Wildcard masks work in reverse logic from subnet masks. When broken out into binary form, a **0** indicates which bits of the IPv4 address to consider, a **1** indicates which bits are disregarded. For example, specifying **255** in any octet of the wildcard mask equates to a “don’t care” for that octet in the IP address. Additionally, a 30-bit mask would be represented with the wildcard string **0.0.0.3**, a 28-bit mask with **0.0.0.15**, a 24-bit mask with **0.0.0.255**, and so forth.

4. Using the keyword **hostname** to match based on a domain naming system (DNS) name. DNS servers must be configured or host names must be locally defined for this function to work.

Step 4:
Apply the created IPv4 ACP to an interface. To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** <*acpv4 name*>. The following example assigns ACP **UNTRUSTED** to the Ethernet 0/1 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip access-policy UNTRUSTED**

ip policy-class *<ipv4 acp name>* max-host-sessions *<number>*

Use the **ip policy-class max-host-sessions** command to create or alter settings for an Internet Protocol version 4 (IPv4) access control policy (ACP). For more details on ACP functionality in AOS, refer to the *IPv4 Access Control Policy Command Set on page 4278*. Use the **no** form of this command to return to the default value.

Syntax Description

<ipv4 acl name>	Identifies the configured IPv4 ACP using an alphanumeric descriptor (maximum of 50 characters). All IPv4 ACP descriptors are case sensitive.
<number>	Specifies the maximum number of allowed IPv4 ACP sessions that can be created from each unique source address. This command is used in conjunction with a named IPv4 ACP and only applies the limit to that particular IPv4 ACP. The number must be within the appropriate range limits. The limits depend on the type of AOS device being used. Setting this value to **0** restores the default setting. By default, this feature is turned off (meaning no limits per source address will be enforced).

Default Values

By default, all AOS security features are disabled and there are no configured ACP entries.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example allows no more than **100** policy sessions to be sourced from a single host IP address on the ACP named **PRIVATE**:

(config)**#ip policy-class PRIVATE max-host-sessions 100**

ip policy-class *<ipv4 acp name>* max-sessions *<number>*

Use the **ip policy-class max-sessions** command to specify the number of allowed sessions for an Internet Protocol version 4 (IPv4) access control policy (ACP). For more details on IPv4 ACP functionality in AOS, refer to the *IPv4 Access Control Policy Command Set on page 4278*. Use the **no** form of this command to return to the default value.

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP using an alphanumeric descriptor (maximum of 50 characters). All ACP descriptors are case sensitive.
<number>	Specifies the maximum number of allowed policy sessions for the named IPv4 ACP. This number must be within the appropriate range limits. The limits depend on the type of AOS device being used. Setting this value to **0** restores the default setting. When setting the **max-sessions** for all IPv4 ACPs, this default is determined at boot time based on the amount of memory available. For a named IPv4 ACP, this default is one-third of the total number of allowed ACP sessions.

Default Values

By default, all AOS security features are disabled and there are no configured ACP entries.

Command History

Release 2.1	Command was introduced.

Functional Notes

To set the system-wide maximum limit for ACP sessions (both IPv4 and IPv6), use the command *policy-class max-sessions <number> on page 1654*. To set the maximum limit for IPv6 ACP sessions, use the command *ipv6 policy-class <ipv6 acp name> max-sessions <number> on page 1550*.

Usage Examples

The following example allows no more than **100** IPv4 policy sessions on the ACP named **PRIVATE**:

(config)**#ip policy-class PRIVATE max-sessions 100**

The following example restores the default policy sessions limit on the ACP named **PRIVATE**:

(config)**#no ip policy-class PRIVATE max-sessions**

ip policy-class *<ipv4 acp name>* rpf-check

Use the **ip policy-class rpf-check** command to verify that Internet Protocol version 4 (IPv4) traffic has entered on the appropriate interface using a route lookup. Reverse path forwarding (RPF) is essentially a spoofing check. For more details on IPv4 policy class functionality in AOS, refer to the *IPv4 Access Control Policy Command Set on page 4278*. Use the **no** form of this command to disable this feature.

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 access control policy (ACP) using an alphanumeric descriptor (maximum of 50 characters). All ACP descriptors are case sensitive.
rpf-check	Enables RPF check (spoofing).

Default Values

This command is enabled by default.

Command History

Release 12.1	Command was introduced.

Functional Notes

The **rpf-check** feature should be disabled if your application allows IPv4 traffic to arrive on an interface sourced from networks contradicting the route table. This feature can be disabled on a per ACP basis by issuing this command in conjunction with the ACP name you do not want to be checked.

Usage Examples

The following example turns off the **rpf-check** feature for the IPv4 ACP named **PRIVATE**:

(config)**#no ip policy-class PRIVATE rpf-check**

ip policy-timeout

Use multiple **ip policy-timeout** command to customize timeout intervals for the established Internet Protocol version 4 (IPv4) firewall sessions. The policy session timeout determines when the time to live (TTL) for the session expires and ends the session. This command configures the policy timeout for the following protocols: (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol version 4 (ICMPv4), Authentication Header (AH) Protocol, generic routing encapsulation (GRE), encapsulating security payload (ESP)) or specific services (by listing the particular port number). Use the **no** form of this command to return to the default timeout values. Variations of this command include:

ip policy-timeout [ahp | esp | gre | icmp] <*timeout*>
ip policy-timeout [tcp | udp] all-ports <*timeout*>
ip policy-timeout [tcp | udp] <*port*> <*timeout*>
ip policy-timeout [tcp | udp] range <*beginning port*> <*ending port*> <*timeout*>

Syntax Description

ahp	Specifies the data protocol as AHP.
esp	Specifies the data protocol as ESP.
gre	Specifies the data protocol as GRE.
icmp	Specifies the data protocol as ICMPv4.
<*timeout*>	Specifies the wait interval (in seconds) before an active session is closed. Valid range is **0** to **4294967295** seconds.
tcp	Specifies the data protocol as TCP. If you are using TCP, you can also specify the timeout for a specific port, a range of ports, or all TCP ports.
udp	Specifies the data protocol as UDP. If you are using UDP, you can also specify the timeout for a specific port, a range of ports, or all UDP ports.
all-ports	Specifies all ports of either TCP or UDP are used if a specific match is not found.
<*port*>	Specifies a single TCP or UDP port. Keywords are available for well-known protocols, as those listed below. Valid port range is **0** to **65535**.
range	Customizes timeout intervals for a range of TCP or UDP ports.
<*beginning port*>/<*ending port*>	Specifies the range of ports, to which to apply the timeout value; valid only for specifying TCP and UDP services. Valid ports range between **0** and **65535**. The following is the list of TCP port numbers that may be identified using the text name (in **bold**): **bgp** (Port 179) **chargen** (Port 19) **cmd** (Port 514) **daytime** (Port 13) **discard** (Port 9) **kshell** (Port 544) **login** (Port 513) **lpd** (Port 515) **nntp** (Port 119) **pim-auto-rp** (Port 496)

domain (Port 53)	**pop2** (Port 109)
echo (Port 7)	**pop3** (Port 110)
exec (Port 512)	**smtp** (Port 25)
finger (Port 79)	**ssh** (Port 22)
ftp (Port 21)	**sunrpc** (Port 111)
ftp-data (Port 20)	**tacacs** (Port 49)
gopher (Port 70)	**talk** (Port 517)
hostname (Port 101)	**telnet** (Port 23)
https (Port 443)	**time** (Port 37)
ident (Port 113)	**uucp** (Port 540)
irc (Port 194)	**whois** (Port 43)
klogin (Port 543)	**www** (Port 80)

The following is the list of UDP port numbers that may be identified using the text name (in **bold**):

biff (Port 512)	**pim-auto-rp** (Port 496)
bootpc (Port 68	**rip** (Port 520)
bootps (Port 67)	**ripng** (Port 521)
discard (Port 9)	**snmp** (Port 161)
dnsix (Port 195)	**snmptrap** (Port 162))
domain (Port 53)	**sunrpc** (Port 111)
echo (Port 7)	**syslog** (Port 514)
isakmp (Port 500)	**tacacs** (Port 49)
mobile-ip (Port 434)	**talk** (Port 517)
nameserver (Port 42)	**tftp** (Port 69)
netbios-dgm (Port 138)	**time** (Port 37)
netbios-ns (Port 137)	**who** (Port 513)
netbios-ss (Port 139)	**xdmcp** (Port 177)
ntp (Port 123)	

<timeout> Specifies the wait interval (in seconds) before an active session is closed. Valid range is **0** to **4294967295** seconds.

Default Values

By default, policy session timeouts are set to **600** seconds for established TCP policy sessions, and **60** seconds for all other protocols.

Command History

Release 2.1	Command was introduced.
Release 11.1	Added AHP, GRE, and ESP policies.
Release 18.2	The **syslog** option for TCP ports was removed.
Release R10.1.0	Command was expanded to include the **ripng** option for UDP ports.

Usage Examples

The following example creates customized policy timeouts for the following:

Internet traffic (TCP Port 80) timeout 24 hours (**86400** seconds)
Telnet (TCP Port 23) timeout 20 minutes (**1200** seconds)
FTP (TCP Port 21) timeout 5 minutes (**300** seconds)
All other TCP services timeout 8 minutes (**480** seconds)

(config)**#ip policy-timeout tcp www 86400**
(config)**#ip policy-timeout tcp telnet 1200**
(config)**#ip policy-timeout tcp ftp 300**
(config)**#ip policy-timeout tcp all-ports 480**

The following example creates customized policy timeouts for UDP network basic input/output system (NetBIOS) ports 137 to 139 of **200** seconds and UDP ports **6000** to **7000** of **300** seconds:

(config)**#ip policy-timeout udp range netbios-ns netbios-ss 200**
(config)**#ip policy-timeout udp range 6000 7000 300**

The following example creates a customized policy timeout of **1200** seconds for ESP:

(config)**#ip policy-timeout esp 1200**

The following example creates a customized policy timeout of **1200** seconds for GRE:

(config)**#ip policy-timeout gre 1200**

The following example creates a customized policy timeout of **1200** seconds for AHP:

(config)**#ip policy-timeout ahp 1200**

ip prefix-list <*name*> description *“<text>”*

Use the **ip prefix-list description** command to create and name prefix lists. Use the **no** form of this command to remove a prefix list.

Syntax Description

<name>	Specifies a particular prefix list.
“<text>”	Assigns text (enclosed in quotation marks) used as a description for the prefix list. Maximum length is 80 characters.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command adds a string of up to 80 characters as a description for a prefix list. It also creates the prefix list if a prefix list of that name does not already exist.

Usage Examples

The following example adds a description to the prefix-list **test**:

(config)**#ip prefix-list test description “An example prefix list”**

ip prefix-list <*name*> seq <*number*>

Use the **ip prefix-list seq** command to specify a prefix to be matched or a range of mask lengths. Use the **no** form of this command to remove a prefix list. Variations of this command include:

ip prefix-list <*name*> **seq** <*number*> **deny** <*network ip /length*>
ip prefix-list <*name*> **seq** <*number*> **deny** <*network ip /length*> **ge** <*value*>
ip prefix-list <*name*> **seq** <*number*> **deny** <*network ip /length*> **le** <*value*>
ip prefix-list <*name*> **seq** <*number*> **permit** <*network ip /length*>
ip prefix-list <*name*> **seq** <*number*> **permit** <*network ip /length*> **ge** <*value*>
ip prefix-list <*name*> **seq** <*number*> **permit** <*network ip /length*> **le** <*value*>

Syntax Description

<*name*>	Specifies a particular prefix list.
<*number*>	Specifies the entry's unique sequence number that determines the processing order. Lower numbered entries are processed first. Range is **1** to **4294967294**.
permit <*network ip /length*>	Permits access to entries matching the specified network IP address and the corresponding network prefix length (for example, **10.10.10.1 /24**).
deny <*network ip /length*>	Denies access to entries matching the specified network IP address and the corresponding network prefix length (for example, **10.10.10.1 /24**).
le <*value*>	Specifies the upper end of the range. Range is **0** to **32**.
ge <*value*>	Specifies the lower end of the range. Range is **0** to **32**.

Default Values

If no ge or le parameters are specified, an exact match is assumed. If only ge is specified, the range is assumed to be from ge-value to 32. If only le is specified, the range is assumed to be from len to le-value.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command specifies a prefix to be matched. If the network address is entered without specifying a range for prefix lengths, the router assumes that the route must be an exact match. For example, if the command **ip prefix-list TEST seq 5 permit 10.1.0.0/16** is entered, the BGP interface will only accept routes to the entire 10.1.0.0 /16 subnet. It will not accept routes to a network, such as 10.1.1.0/ 24, which was subdivided from the /16 network.

Optionally, this command may specify a range of mask lengths. The following rule must be followed: len < ge-value $\leq$ le-value. A filter that exactly matches a prefix length can be created by entering the length for both the **ge** and **le** values. A prefix list with no entries allows all routes. A route that does not match any entries in a prefix list is dropped. As soon as a route is permitted or denied, there is no further processing of the rule in the prefix list. A route that is denied at the beginning entry of a prefix list will not be allowed, even if it matches a permitting entry further down the list.

Usage Examples

The following example creates a prefix list entry in the prefix list TEST that allows all routes to subnets in the 10.1.0.0 /16 network with a prefix length up to and including 24:

(config)**#ip prefix-list TEST seq 5 permit 10.1.0.0/16 le 24**

The following example creates a prefix list entry in the prefix list TEST that allows any route to a /24 subnet in the 10.1.0.0 /16 range, but rejects routes destined for the entire 10.1.0.0 /16 network:

(config)**#ip prefix-list TEST seq 5 permit 10.1.0.0/16 ge 24 le 24**

ip radius source-interface <*interface*>

Use the **ip radius source-interface** command to specify the network attached storage (NAS) IP address attribute passed with the remote authentication dial-in user service (RADIUS) authentication request packet. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the configuration to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the configuration to the default unnamed VRF. Use the **no** form of this command to remove a defined source interface. Variations of this command include:

ip radius source-interface <*interface*>
ip radius vrf <*name*> **source-interface** <*interface*>

Syntax Description

<*interface*>	Specifies the source interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip radius source-interface ?** for a complete list of interfaces.
vrf <*name*>	Specifies the name of the VRF to which to assign the attribute.

Default Values

By default, no source interface is defined.

Command History

Release 5.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 15.1	Command was expanded to include the bridged virtual interface (BVI).
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

If this value is not defined, the address of the source network interface is used.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example configures the Ethernet 0/1 port to be the source interface:

(config)**#ip radius source-interface ethernet 0/1**

The following example configures the BVI 1 interface to be the source interface:

(config)**#ip radius source-interface bvi 1**

The following example configures the Ethernet 0/1 port to be the source interface:

(config)**#ip radius vrf RED source-interface ethernet 0/1**

The following example configures the BVI 1 interface to be the source interface:

(config)**#ip radius vrf RED source-interface bvi 1**

ip route

Use the **ip route** command to add an Internet Protocol version 4 (IPv4) static route to the IPv4 route table. Use the **no** form of this command to remove a configured IPv4 static route. Variations of this command include:

ip route <*ip address*> <*subnet mask*> <*interface*>
ip route <*ip address*> <*subnet mask*> <*interface*> <*administrative distance*>
ip route <*ip address*> <*subnet mask*> <*interface*> <*administrative distance*> **tag** <*number*>
ip route <*ip address*> <*subnet mask*> <*interface*> <*administrative distance*> **track** <*name*>
ip route <*ip address*> <*subnet mask*> <*interface*> <*administrative distance*> **track** <*name*> **tag** <*number*>
ip route <*ip address*> <*subnet mask*> <*interface*> **tag** <*number*>
ip route <*ip address*> <*subnet mask*> <*ip address*>
ip route <*ip address*> <*subnet mask*> <*ip address*> **tag** <*number*>
ip route <*ip address*> <*subnet mask*> <*ip address*> **track** <*name*>
ip route <*ip address*> <*subnet mask*> <*ip address*> **tag** <*number*> **track** <*name*>
ip route <*ip address*> <*subnet mask*> <*ip address*> <*administrative distance*>
ip route <*ip address*> <*subnet mask*> <*ip address*> <*administrative distance*> **tag** <*number*>
ip route <*ip address*> <*subnet mask*> <*ip address*> <*administrative distance*> **track** <*name*>
ip route <*ip address*> <*subnet mask*> <*ip address*> <*administrative distance*> **track** <*name*> **tag** <*number*>
ip route <*ip address*> <*subnet mask*> **null 0**
ip route <*ip address*> <*subnet mask*> **null 0** <*administrative distance*>
ip route <*ip address*> <*subnet mask*> **null 0** <*administrative distance*> **tag** <*number*>
ip route <*ip address*> <*subnet mask*> **null 0** <*administrative distance*> **track** <*name*>
ip route <*ip address*> <*subnet mask*> **null 0 tag** <*number*>
ip route <*ip address*> <*subnet mask*> **null 0 track** <*name*>

Syntax Description

<*ip address*>	Specifies the IPv4 network address to add to the route table. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
[<*interface*> **|** <*ip address*>**]**	Specifies the far-end IPv4 address or an egress interface in the unit. Use the **ip route** <*ip address*> <*subnet mask*> **?** command to display a complete list of egress interfaces.
null 0	Optional. Specifies that traffic is routed to the null interface. The router drops all packets destined for the null interface. Use the null interface to allow the router to advertise a route, but not forward traffic to the route.
<*administrative distance*>	Optional. Specifies an administrative distance associated with a particular router used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more preferable the route. Range is **1** to **255**.

tag <*number*>	Optional. Specifies a number to use as a tag for this route. Route tags are used to label and filter routes when dynamically redistributing routes into a routing protocol (such as Routing Information Protocol (RIP)/open shortest path first (OSPF)/Border Gateway Protocol (BGP)). Range is **1** to **65535**.
track <*name*>	Optional. Enables tracking on the indicated route. Once the named track enters a fail state, the route specified by the command is disabled and traffic will no longer be routed using that route. For more information on configuring tracks, refer to *track <name> on page 1886*.

Default Values

By default, there are no configured routes in the route table, and the tag of 0 is applied to the route.

Command History

Release 1.1	Command was introduced.
Release 9.1	Tunnel was added as a supported interface.
Release 11.1	Demand was added as a supported interface.
Release 13.1	Command was expanded to include the **track** feature.
Release 15.1	Command was expanded to include route tagging capability.

Usage Examples

The following example adds an IPv4 static route to the **10.220.0.0 /16** network through the next-hop router **192.22.45.254** and an IPv4 default route to **175.44.2.10**:

(config)**#ip route 10.220.0.0 255.255.0.0 192.22.45.254**
(config)**#ip route 0.0.0.0 0.0.0.0 175.44.2.10**

ip route vrf

Use the **ip route vrf** command to create an Internet Protocol version 4 (IPv4) static route in one of the nondefault virtual routing and forwarding (VRF) instances. Use the **no** form of this command to remove the static route. Variations of this command include:

ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]**
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** *<distance>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** *<distance>* **tag** *<number>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** *<distance>* **tag** *<number>* **track** *<name>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** *<distance>* **track** *<name>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** *<distance>* **track** *<name>* **tag** *<number>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** **tag** *<number>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** **tag** *<number>* **track** *<name>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** **track** *<name>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **[***<interface>* **|** *<ipv4 address>***]** **track** *<name>* **tag** *<number>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **null 0**
ip route vrf *<name> <ipv4 address> <subnet mask>* **null 0** *<distance>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **null 0** *<distance>* **tag** *<number>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **null 0** *<distance>* **track** *<name>*
ip route vrf *<name> <ip4v address> <subnet mask>* **null 0 tag** *<number>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **null 0 tag** *<number>* **track** *<name>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **null 0 track** *<name>*
ip route vrf *<name> <ipv4 address> <subnet mask>* **null 0 track** *<name>* **tag** *<number>*

Syntax Description

<name>	Specifies the name of the VRF instance.
<ipv4 address>	Specifies the network address to add to the route table. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). Valid prefix lengths are 0 to 32.
[*<interface>* **|** *<ipv4 address>***]**	Specifies the far-end IPv4 address or an egress interface in the unit. Use the **ip route** *<ipv4 address> <subnet mask>* **?** command to display a complete list of egress interfaces. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

null 0	Optional. Routes traffic destined for the specified network to the null interface. The router drops all packets destined for the null interface. Use the null interface to allow the router to advertise a route, but not forward traffic to the route.
<distance>	Optional. Specifies an administrative distance associated with a particular router used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more preferable the route. Range is **1** to **255**.
track *<name>*	Optional. Enables tracking on the indicated route. Once the named track enters a fail state, the route specified by the command is disabled and traffic will no longer be routed using that route. For more information on configuring tracks, refer to *track <name> on page 1886*.
tag *<number>*	Optional. Specifies a number to use as a tag for this route. Route tags are used to label and filter routes when dynamically redistributing routes into a routing protocol (such as Routing Information Protocol (RIP)/open shortest path first (OSPF)/Border Gateway Protocol (BGP)). Range is **1** to **65535**.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

The VRF must have already been created (using the command *vrf <name> route-distinguisher on page 1989*) before static routes can be configured.

Usage Examples

The following example adds a static route to the routing and forwarding tables used for the VRF **RED**:

(config)**#ip route vrf RED 10.220.0.0 255.255.0.0 192.22.45.254**
(config)**#ip route vrf RED 0.0.0.0 0.0.0.0 175.44.2.10**

ip route-cache express

Use the **ip route-cache express** command to globally enable Layer 3 switching. Use the **no** form of this command to disable Layer 3 switching.

Syntax Description

No subcommands.

Default Values

Layer 3 switching is disabled by default, except on the NetVanta 1544. Layer 3 switching is enabled by default on the NetVanta 1544.

Functional Notes

Layer 3 switching cannot be disabled on the NetVanta 1544. For more information about Layer 3 switching, refer to the *Layer 3 Switching in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example globally enables Layer 3 switching:

(config)**#ip route-cache express**

ip route vrf

Use the **ip route vrf** command to create an Internet Protocol version 4 (IPv4) static route in one of the nondefault virtual routing and forwarding (VRF) instances. Use the **no** form of this command to remove the static route. Variations of this command include:

ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]**
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** <*distance*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** <*distance*> **tag** <*number*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** <*distance*> **tag** <*number*> **track** <*name*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** <*distance*> **track** <*name*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** <*distance*> **track** <*name*> **tag** <*number*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** **tag** <*number*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** **tag** <*number*> **track** <*name*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** **track** <*name*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **[**<*interface*> **|** <*ipv4 address*>**]** **track** <*name*> **tag** <*number*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0**
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0** <*distance*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0** <*distance*> **tag** <*number*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0** <*distance*> **track** <*name*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0 tag** <*number*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0 tag** <*number*> **track** <*name*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0 track** <*name*>
ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **null 0 track** <*name*> **tag** <*number*>

Syntax Description

<*name*>	Specifies the name of the VRF instance.
<*ipv4 address*>	Specifies the network address to add to the route table. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). Valid prefix lengths are 0 to 32.
[<*interface*> **|** <*ipv4 address*>**]**	Specifies the far-end IPv4 address or an egress interface in the unit. Use the **ip route** <*ipv4 address*> <*subnet mask*> **?** command to display a complete list of egress interfaces. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

null 0	Optional. Routes traffic destined for the specified network to the null interface. The router drops all packets destined for the null interface. Use the null interface to allow the router to advertise a route, but not forward traffic to the route.
<distance>	Optional. Specifies an administrative distance associated with a particular router used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more preferable the route. Range is **1** to **255**.
track *<name>*	Optional. Enables tracking on the indicated route. Once the named track enters a fail state, the route specified by the command is disabled and traffic will no longer be routed using that route. For more information on configuring tracks, refer to *track <name> on page 1886*.
tag *<number>*	Optional. Specifies a number to use as a tag for this route. Route tags are used to label and filter routes when dynamically redistributing routes into a routing protocol (such as Routing Information Protocol (RIP)/open shortest path first (OSPF)/Border Gateway Protocol (BGP)). Range is **1** to **65535**.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release 17.5	Command was expanded to include the loopback interface.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

The VRF must have already been created (using the command *vrf <name> route-distinguisher on page 1989*) before static routes can be configured.

Usage Examples

The following example adds a static route to the routing and forwarding tables used for the VRF **RED**:

(config)**#ip route vrf RED 10.220.0.0 255.255.0.0 192.22.45.254**
(config)**#ip route vrf RED 0.0.0.0 0.0.0.0 175.44.2.10**

ip routing

Use the **ip routing** command to enable the AOS IP routing functionality. Use the **no** form of this command to disable IP routing.

Syntax Description

No subcommands.

Default Values

By default, IP routing is enabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the AOS IP routing functionality:

(config)**#ip routing**

ip rtp dtmf-relay min-duration <*value*>

Use the **ip rtp dtmf-relay min-duration** command to configure dual tone multi-frequency (DTMF) relay duration that the DTMF digits must receive in order to be relayed. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies timeout period (in multiples of 10 milliseconds) allowed for DTMF relay duration. Range is **20** to **250** seconds.

Default Values

By default, the DTMF relay value is **30**.

Command History

Release A2	Command was introduced.

Usage Examples

The following example sets the DTMF relay duration to **50**:

(config)**#ip rtp dtmf-relay min-duration 50**

ip rtp firewall-traversal

Use the **ip rtp firewall-traversal** command to enable dynamic firewall traversal capability for RTP-based traffic, allowing deep packet inspection of Session Description Protocol (SDP) packets to occur so RTP will correctly traverse network address translation (NAT) in the firewall. This will open the proper ports dynamically for the RTP traffic. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip rtp firewall-traversal
ip rtp firewall-traversal <*start udp port*>
ip rtp firewall-traversal <*start udp port*> <*end udp port*>
ip rtp firewall-traversal enforce-symmetric-ip
ip rtp firewall-traversal policy-timeout <*value*>
ip rtp firewall-traversal reuse-nat-ports

Syntax Description

<*end udp port*>	Specifies the ending User Datagram Protocol (UDP) port to reserve for NAT. Range is **2001** to **65535**.
<*start udp port*>	Specifies the starting UDP port to reserve for NAT. Range is **2000** to **65534**.
enforce-symmetric-ip	Optional. Specifies that the same IP address must be used for both transmit and receive for the RTP stream.
policy-timeout <*value*>	Optional. Specifies timeout period in seconds allowed for inactive RTP sessions to remain in the firewall. Range is **1** to **4294967295** seconds.
reuse-nat-ports	Optional. Specifies that NAT ports be reused during calls.

Default Values

By default, the RTP dynamic firewall traversal is disabled and the policy timeout period is **45** seconds.

By default, when the RTP dynamic firewall traversal is enabled for AOS voice products, the UDP starting port is **50000**, and the ending UDP port is **52999**. If no range is specified, the default range is **3000**, unless the starting port is equal to or greater than **62538**, in which case the range will be reduced such that the ending port is **65535**.

Command History

Release 10.1	Command was introduced.
Release 14.1	Command was updated to include the **reuse-nat-ports** option.
Release A2	Command was updated to include the **enforce-symmetric-ip** option.
Release 18.2	Command was updated to include the <*start udp port*> and <*end udp port*> variables.
Release A5.01	Command was updated to include the <*start udp port*> and <*end udp port*> variables for SIP RTP packets on AOS voice products, and the associated voice product defaults.

Functional Notes

Session Initiation Protocol (SIP) uses the SDP to format the SIP message body in order to negotiate a Realtime Transport Protocol (RTP)/Realtime Transport Control Protocol (RTCP) connection between two or more user agents (UAs). The ports used for this will always be selected in a pair, with the even port used for RTP and the odd port for RTCP.

You can also specify which range of NAT UDP ports are reserved for use only for SIP RTP packets using the *<start udp port> <end udp port>* parameters of this command.

The SIP application-level gateway (ALG) (enabled using the **ip firewall alg sip** command) configures the firewall to examine the ALL SIP packets it identifies and maintain knowledge of SIP transmissions on the network. Since SIP packet headers include port information for the call setup, the ALG must intelligently read the packets and remember the information.

For a full SIP implementation, dynamic firewall traversal for RTP traffic must also be enabled using the **ip rtp firewall-traversal** command. This allows the firewall to open the proper ports for the RTP traffic between UAs. For more details on SIP functionality in AOS, refer to the *Functional Notes* and *Technology Review* sections of the command *ip firewall alg on page 1373*.

Usage Examples

The following example enables dynamic firewall traversal, and sets the policy timeout period at **60** seconds:

(config)**#ip rtp firewall-traversal policy-timeout 60**

ip rtp media-anchoring

Use the **ip rtp media-anchoring** command to enable media anchoring for all Realtime Transport Protocol (RTP) calls. Use the **no** form of this command to return to the default setting.

ip rtp media-anchoring
ip rtp media-anchoring qos dscp <*value*>
ip rtp media-anchoring session timeout <*value*>

Syntax Description

qos dscp <*value*>	Specifies the differentiated services code point (DSCP) value for media-anchoring quality of service (QoS) settings. Range is **0** to **63**.
session timeout <*value*>	Specifies the timeout period, in seconds, of an anchoring association after the associated RTP packet flow ends. Range is **32** to **900** seconds.

Default Values

By default, media anchoring is disabled. If media anchoring is enabled, the default **session timeout** value is **45** seconds.

Command History

Release R10.1.0	Command was introduced.
Release R10.5.0	Command was expanded to include the **qos dscp** parameter.

Usage Examples

The following example sets the media anchoring session timeout period at **60** seconds:

(config)**#ip rtp media-anchoring session timeout 60**

Technology Review

Media anchoring, through the use of Session Description Protocol (SDP) manipulation, directs all RTP packets generated in the local network to the media anchoring device (an AOS unit with media anchoring enabled). Outgoing RTP packets (which contain the source IP address and port number of an Internet Protocol (IP) private branch exchange (PBX) or phone and the destination IP address and port of the media anchoring device) are modified to be sourced from the gateway and destined to the public network. The process is reversed for incoming RTP packets.

When a local Voice over Internet Protocol (VoIP) phone makes a call to the public network, the local network will be configured to have all SIP messages routed to the media anchoring device. The media anchoring device will receive a Session Initiation Protocol (SIP) packet with an SDP offer from the IP phone when the phone tries to make the call.

If media anchoring is enabled, the media anchoring device will, based on the SDP offer, determine the egress interface for relaying the SDP to the public network and substitute the IP address of that interface for the connection information IP address contained in the original SDP offer. Additionally, it will substitute a port number in the media anchoring range (User Datagram Protocol (UDP) 10000 and above) in any media descriptions. The offer will then be relayed on the appropriate outbound SIP trunk. This will cause RTP from the public endpoint to be routed to the media anchoring device instead of the VoIP phone.

When the media anchoring device receives the SDP answer from the destination endpoint, the connection information IP address and media description UDP port numbers will be replaced with the IP address of the interface for which the SDP answer was originally destined (i.e., the interface on which the VoIP phone is reachable) and a second port number within the media anchoring UDP port range. This will cause RTP from the VoIP phone to be routed to the media anchoring device instead of the public network.

When the RTP session begins, packets inbound from the public network will have the far-end IP address as the source and the media anchoring device as the destination. The anchoring implementation will replace the source address with the IP address of the egress (to the IP phone) interface on the media anchoring device, and it will replace the destination address with that of the VoIP phone. This information is derived from the UDP port on which the packet was originally received from the network because the anchoring implementation stored this information when the port was allocated.

The same operation will occur on packets inbound from the IP phone. These packets will have the IP phone's IP address and UDP port as the source and the media anchoring device as the destination. The source IP address will be changed to that of the egress (to the public network) interface on the media anchoring device, and the port will be changed to the anchoring port established when the SDP offer was originally manipulated. The destination IP address and UDP port will be changed to that of the public network endpoint.

ip rtp media-anchoring transcoding codec

Use the **ip rtp media-anchoring transcoding codec** command to enable coder/decoder (CODEC) transcoding globally for all Session Initiation Protocol (SIP) endpoints on an AOS session border controller (SBC) device. Use the **no** form of this command to disable the CODEC transcoding feature.

Syntax Description

No subcommands.

Default Values

By default, CODEC transcoding is disabled.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

Before CODEC transcoding can be enabled, media anchoring must be enabled. Refer to the command *ip rtp media-anchoring on page 1458* for more information.

In addition, to configure transcoding you must specify the CODEC settings for each SIP endpoint. Refer to the following sections in this guide for more information: *Voice CODEC List Command Set on page 4893*, *Voice T1 Trunk Command Set on page 5151*, *Voice SIP Trunk Command Set on page 5052*, or *Voice ISDN Trunk Command Set on page 5008*

Usage Examples

The following example enables CODEC transcoding globally on the AOS device:

(config)**#ip rtp media-anchoring transcoding codec**

ip rtp media-anchoring transcoding dtmf

Use the **ip rtp media-anchoring transcoding dtmf** command to enable dualtone multifrequency (DTMF) signal transcoding on a global basis for all Session Initiation Protocol (SIP) endpoints connected to the AOS session border controller (SBC) device. Use the **no** form of this command to disable the DTMF transcoding feature.

Syntax Description

No subcommands.

Default Values

By default, DTMF transcoding is disabled.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

Before DTMF transcoding can be enabled, media anchoring must be enabled. Refer to the command *ip rtp media-anchoring on page 1458* for more information.

In addition, to configure transcoding you must specify the DTMF settings for each SIP endpoint. Refer to the following sections in this guide for more information: *Voice T1 Trunk Command Set on page 5151*, *Voice SIP Trunk Command Set on page 5052*, or *Voice ISDN Trunk Command Set on page 5008*.

Usage Examples

The following example enables DTMF transcoding globally on the AOS device:

(config)**#ip rtp media-anchoring transcoding dtmf**

ip rtp nat-session timeout *<value>*

Use the **ip rtp nat-session timeout** command to configure the network address translation (NAT) session timeout for the Realtime Transport Protocol (RTP) packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the timeout period in seconds allowed for an inactive NAT session. Range is **32** to **900** seconds.

Default Values

By default, the timeout period is **32** seconds.

Command History

Release A2.03	Command was introduced.

Usage Examples

The following example sets the NAT session timeout period at **60** seconds:

(config)**#ip rtp nat-session timeout 60**

ip rtp nat-table-timeout <*value*>

Use the **ip rtp nat-table timeout** command to configure the network address translation (NAT) table timeout for the Realtime Transport Protocol (RTP) packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the timeout period in seconds allowed for an inactive NAT session. Range is **32** to **900** seconds.

Default Values

By default, the timeout period is **32** seconds.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the NAT session timeout period at **60** seconds:

(config)**#ip rtp nat-session timeout 60**

ip rtp qos dscp *<value>*

Use the **ip rtp qos dscp** command to configure the differentiated services code point (DSCP) value with which to mark IP Realtime Transport Protocol (RTP) packets. This marking can then be used by the quality of service (QoS) mechanisms to give priority for this type of traffic in the unit. Use the **no** form of this command to disable this feature.

Syntax Description

<value>	Specifies the DSCP value. Valid range is **0** to **63**.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the DSCP value to **63**:

(config)**#ip rtp qos dscp 63**

ip rtp quality-monitoring

Use the **ip rtp quality-monitoring** command to globally enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets. Use the **no** form of this command to disable VQM. Variations of this command include:

ip rtp quality-monitoring
ip rtp quality-monitoring scoring-adjustment japan
ip rtp quality-monitoring sip
ip rtp quality-monitoring udp

Syntax Description

scoring-adjustment japan	Optional. Sets the region for scoring adjustment for Japan. In Japan, the mean opinion score (MOS) statistics are calculated differently than in other regions. VQM must be disabled and then enabled again for this setting to take effect.
sip	Optional. Specifies that Session Initiation Protocol (SIP) is the signaling type of the RTP stream to monitor.
udp	Optional. Specifies that User Datagram Protocol (UDP) is the signaling type of the RTP stream to monitor.

Default Values

By default, the VQM is disabled globally.

Functional Notes

Disabling VQM on the global level (for example, to change the scoring adjustment) erases all active calls, new calls, and interface statistics. Call history and endpoint statistics are not affected.

If the **sip** or **udp** parameters are specified, and VQM has not previously been enabled at the global level, VQM will be enabled globally. Enabling UDP packet inspection forces the AOS unit to inspect every UDP packet to determine if it is an RTP packet, placing a significant load on the AOS unit. UDP packet inspection should only be enabled if IP phones are being used and they do not pass through the SIP ALG, SIP proxy, or SIP B2BUA.

For more information about VQM configuration, refer to the configuration guide *Configuring VQM in AOS* available online at https://supportcommunity.adtran.com.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring at the global level and does not specify a scoring region or RTP signaling type:

(config)**#ip rtp quality-monitoring**

ip rtp quality-monitoring filter

Use the **ip rtp quality-monitoring filter** command to filter the number of Realtime Transport Protocol (RTP) voice streams monitored by voice quality monitoring (VQM). Use the **no** form of this command to remove the filter. Variations of this command include:

ip rtp quality-monitoring filter user <*user*>
ip rtp quality-monitoring filter access-class <*name*>

Syntax Description

user <*user*>	Specifies that only calls from certain users are measured. Users are specified by Session Initiation Protocol (SIP) To or From headers, in the format **user@host**. Multiple users can be monitored simultaneously.
access-class <*name*>	Specifies that only RTP streams that match the previously configured access control list (ACL) are measured. The <*name*> parameter is the ACL to be used. Only one ACL can be applied to VQM at a time.

Default Values

By default, VQM is not filtered by user or ACL.

Command History

Release A1	Command was introduced.

Usage Examples

The following example specifies that VQM only monitor RTP streams that match the previously configured ACL, **4thFloorUsers**:

(config)**#ip rtp quality-monitoring filters access-class 4thFloorUsers**

ip rtp quality-monitoring history

Use the **ip rtp quality-monitoring history** commands to configure the call history storage for voice quality monitoring (VQM). You can use this command variations to configure the size of the call history and to specify the thresholds used to decide when calls are stored in the call history. Using the **no** forms of these commands return the call history parameters to the default settings. Variations of this command include:

ip rtp quality-monitoring history cq-mos <*value*>
ip rtp quality-monitoring history jitter <*value*>
ip rtp quality-monitoring history loss <*value*>
ip rtp quality-monitoring history lq-mos <*value*>
ip rtp quality-monitoring history max-streams <*number*>
ip rtp quality-monitoring history out-of-order <*value*>
ip rtp quality-monitoring history pq-mos <*value*>

Syntax Description

cq-mos <*value*>	Specifies a threshold for the conversational quality (CQ) mean opinion score (MOS), and stores statistics below this threshold. The range is **0** to **4.4**.
jitter <*value*>	Specifies a threshold for the jitter. Statistics above this threshold are stored as jitter. The packet-to-packet delay variation is measured in milliseconds (from nAvgPDV). The range is **0** to **30000**.
loss <*value*>	Specifies a threshold for loss (in packets). Statistics above this threshold is stored as lost packets. The range is **0** to **30000**.
lq-mos <*value*>	Specifies a threshold for the listening quality (LQ) MOS, and stores statistics below this threshold. The range is **0** to **4.4**.
max-streams <*number*>	Specifies a number of previously completed call statistics to store. This is a count of Realtime Transport Protocol (RTP) streams; each call can contain two RTP streams. The range is **0** to **2000**.
out-of-order <*value*>	Specifies a threshold for out-of-order packets to be logged. Statistics above this threshold are stored. The range is **0** to **30000**.
pq-mos <*value*>	Specifies a threshold for LQ MOS normalized to the PESQ (PQ) scale, and stores statistics below this threshold. The range is **0** to **4.4**.

Default Values

By default, the maximum number of RTP streams allowed in the history is **100**.

Setting the size of the call history to a large number can result in the AOS unit running out of memory.

By default, MOS thresholds are set to **4.4**, and jitter, loss, and out-of-order packet thresholds are set to **0**.

Command History

Release 17.1	Command was introduced.

Functional Notes

As calls complete, settings configured using this command are examined to determine whether the call should be stored in the call history. The maximum number of streams to store may be configured; newer calls will replace the oldest calls when the call history is full. The MOS, loss, out-of-order packets, and jitter can also be examined when a call completes. By default, all calls are stored in the call history. However, if threshold values are changed from their defaults, only calls with poorer quality than these nondefault thresholds will be stored.

Usage Examples

The following example enables RTP quality monitoring history to store a maximum of **250** RTP streams:

(config)**#ip rtp quality-monitoring history max-streams 250**

ip rtp quality-monitoring jitter-buffer

Use the **ip rtp quality-monitoring jitter-buffer** command to specify the jitter buffer type and configuration for the jitter buffer emulator (JBE) that generates the observable jitter statistics in Realtime Transport Protocol (RTP) quality monitoring. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip rtp quality-monitoring jitter-buffer
ip rtp quality-monitoring jitter-buffer adaptive min <*delay*> **nominal** <*value*>
ip rtp quality-monitoring jitter-buffer adaptive min <*delay*> **nominal** <*value*> **max** <*value*>
ip rtp quality-monitoring jitter-buffer fixed nominal <*value*> **jitter-buffer-size** <*value*>

Syntax Description

adaptive min <*delay*>	Optional. Specifies the minimum acceptable jitter buffer delay to be used by the JBE. The range is **10** to **240** milliseconds.
nominal <*value*>	Optional. Specifies the starting delay applied to packets of the emulated jitter buffer. The range is **10** to **240** milliseconds.
max <*value*>	Optional. Specifies the maximum delay that the adaptive jitter buffer will be allowed to use. The range is **40** to **320** milliseconds.
fixed nominal <*value*>	Optional. Specifies the actual fixed delay that would be applied to the packet in a nonemulated jitter buffer. The range is **4** to **250** milliseconds. There is no default setting.
jitter-buffer-size <*value*>	Optional. Specifies the number of packets that the emulated jitter buffer can hold. The range is **10** to **500** packets. There is no default setting.

Default Values

By default, the jitter buffer is set to **adaptive min 10 nominal 50 max 200**.

Command History

Release 17.1	Command was introduced.
Release A1	Command was introduced in the AOS voice products.
Release A4.01	Command was modified to allow specifying the **nominal** value without specifying the **max** value.

Usage Examples

The following example enables the JBE to hold up to **175** packets in fixed mode:

(config)**#ip rtp quality-monitoring jitter-buffer fixed nominal 50 jitter-buffer-size 175**

ip rtp quality-monitoring jitter-threshold

Use the **ip rtp quality-monitoring jitter-threshold** command to specify the jitter thresholds for the voice quality monitoring (VQM) simulated jitter buffer. These thresholds determine when packets are considered either too early or too late for the jitter buffer window, and are then marked as discarded packets. Changing the jitter threshold will not impact currently active calls, only the calls placed after the configuration change has taken place. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip rtp quality-monitoring jitter-threshold early <*value*>
ip rtp quality-monitoring jitter-threshold late <*value*>

Syntax Description

early <*value*>	Specifies the time by which packets are deemed to have arrived early. The range is **0** to **1000** ms.
late <*value*>	Specifies the time by which packets are deemed to have arrived late. The range is **0** to **1000** ms.

Default Values

By default, jitter thresholds are set to **early 10**, and **late 60**.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example specifies the late jitter threshold at **45** ms:

(config)**#ip rtp quality-monitoring jitter-threshold late 45**

p rtp quality-monitoring reporter <*name*>

Use the **ip rtp quality-monitoring reporter** command to create and name a voice quality monitoring (VQM) reporter. Use the **no** form of this command to delete the reporter. Variations of this command include:

ip rtp quality-monitoring reporter <*name*>
ip rtp quality-monitoring reporter <*name*> **vrf** <*name*>

Syntax Description

<*name*>	Specifies the name of the VQM reporter.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to enable the VQM reporter. If no VRF is specified, the VQM reporter is enabled on the default unnamed VRF instance.

Default Values

By default, no VQM reporter exists.

Command History

Release 17.6	Command was introduced.
Release R13.10.0	Command was expanded to include the **vrf** parameter.

Functional Notes

The **ip rtp quality-monitoring reporter** command creates a VQM reporter and also enters the reporter's configuration mode. For more information on configuring VQM reporters, refer to the *VQM Reporter Command Set on page 4945*.

Usage Examples

The following example creates the VQM reporter **Reporter1** and enters the reporter's configuration mode:

```
(config)#ip rtp quality-monitoring reporter Reporter1
    Configuring New Reporter "Reporter1"
(config-rtp-reporter-Reporter1)#
```


ip rtp quality-monitoring round-trip-delay

Use the **ip rtp quality-monitoring round-trip-delay** command to enable packet round-trip calculations for voice quality monitoring (VQM) and to specify the type of round-trip delay testing. Use the **no** form of this command to disable VQM round-trip delay calculations. Variations of this command include:

ip rtp quality-monitoring round-trip-delay icmp-ping
ip rtp quality-monitoring round-trip-delay icmp-timestamp

Syntax Description

icmp-ping	Specifies the use of Internet Control Message Protocol (ICMP) requests for calculating round-trip delay.
icmp-timestamp	Specifies the use of ICMP timestamp requests for calculating round-trip delay.

Default Values

By default, the calculation type is **icmp-ping**.

Functional Notes

Round-trip delay settings appear in the VQM statistics; however, if Realtime Transport Protocol (RTP) extended reports (RTCP XR) are also available, the received RTCP XR reports supersede the round-trip delay settings.

The endpoints and local units must be synchronized (time and date) for the timestamp method to be accurate. In addition, any firewalls between the voice endpoints must be configured to allow ICMP traffic to pass.

For more information about VQM round-trip delay calculations, and VQM configuration, refer to the configuration guide *Configuring VQM in AOS* available online at https://supportcommunity.adtran.com.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example specifies timestamp requests are used to determine round-trip delay:

(config)**#ip rtp quality-monitoring round-trip-delay icmp-timestamp**

ip rtp quality-monitoring sample one-out-of <*number*>

Use the **ip rtp quality-monitoring sample one-out-of** command to limit the number of Realtime Transport Protocol (RTP) streams monitored by voice quality monitoring (VQM). Use the **no** form of this command to disable VQM sampling.

Syntax Description

<*number*>	Specifies the VQM jitter buffer sampling rate, which causes VQM to only monitor 1 out of the specified number of RTP streams. Range is **1** to **100**.

Default Values

By default, the VQM sampling rate is set to **1**, which means that all RTP streams are monitored.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example specifies that VQM monitors 10 percent of all streams (one out of every **10**):

(config)**#ip rtp quality-monitoring sample one-out-of 10**

ip rtp quality-monitoring snmp trap

Use the **ip rtp quality-monitoring snmp trap** command to configure the Simple Network Management Protocol (SNMP) trap parameters of voice quality monitoring (VQM). Using the **no** form of this command disables VQM SNMP trap reports and collections. Variations of this command include:

ip rtp quality-monitoring snmp trap
ip rtp quality-monitoring snmp trap priority-level error
ip rtp quality-monitoring snmp trap priority-level info
ip rtp quality-monitoring snmp trap priority-level notice
ip rtp quality-monitoring snmp trap priority-level warning

Syntax Description

priority-level	**Optional.** Specifies the priority level of the SNMP trap created by VQM.
error	Specifies that an SNMP trap is created when VQM detects an error event.
info	Specifies that an SNMP trap is created when VQM detects an info event.
notice	Specifies that an SNMP trap is created when VQM detects a notice event.
warning	Specifies that an SNMP trap is created when VQM detects a warning.

Default Values

By default, SNMP traps are not enabled for VQM.

Command History

Release 17.6	Command was introduced.

Usage Examples

The following example enables SNMP traps for VQM:

(config)**#ip rtp quality-monitoring snmp trap**

ip rtp quality-monitoring threshold jitter

Use the **ip rtp quality-monitoring threshold jitter** command to specify the threshold values for logging jitter events during voice quality monitoring (VQM). When more jitter is detected in the Realtime Transport Protocol (RTP) than the specified event threshold, an event message is generated. Use the **no** form of this command to disable the event reporting for that message type and threshold. Variations of this command include:

ip rtp quality-monitoring threshold jitter error
ip rtp quality-monitoring threshold jitter error <*value*>
ip rtp quality-monitoring threshold jitter info
ip rtp quality-monitoring threshold jitter info <*value*>
ip rtp quality-monitoring threshold jitter notice
ip rtp quality-monitoring threshold jitter notice <*value*>
ip rtp quality-monitoring threshold jitter warning
ip rtp quality-monitoring threshold jitter warning <*value*>

Syntax Description

error	Specifies the threshold for jitter error messages to be logged.
info	Specifies the threshold for jitter information messages to be logged.
notice	Specifies the threshold for jitter notice messages to be logged.
warning	Specifies the threshold for jitter warning messages to be logged.
<*value*>	Optional. The range is **0** to **30000**.

Default Values

By default, the jitter logging thresholds are **info 0**, **notice 250**, **warning 350**, and **error 450**.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables VQM jitter warning messages to be logged if jitter occurs above **200** ms:

(config)**#ip rtp quality-monitoring threshold jitter warning 200**

ip rtp quality-monitoring threshold loss

Use the **ip rtp quality-monitoring threshold loss** command to specify the threshold values for logging packet loss events during voice quality monitoring (VQM). When more loss is detected in the Realtime Transport Protocol (RTP) than the specified event threshold, an event message is generated. Use the **no** form of this command disables the event reporting for that message type and threshold. Variations of this command include:

ip rtp quality-monitoring threshold loss error
ip rtp quality-monitoring threshold loss error <*value*>
ip rtp quality-monitoring threshold loss info
ip rtp quality-monitoring threshold loss info <*value*>
ip rtp quality-monitoring threshold loss notice
ip rtp quality-monitoring threshold loss notice <*value*>
ip rtp quality-monitoring threshold loss warning
ip rtp quality-monitoring threshold loss warning <*value*>

Syntax Description

error	Specifies the threshold for lost packets error messages to be logged.
info	Specifies the threshold for lost packets information messages to be logged.
notice	Specifies the threshold for lost packets notice messages to be logged.
warning	Specifies the threshold for lost packets warning messages to be logged.
<*value*>	Optional. The range is **0** to **30000**.

Default Values

By default, the lost packets thresholds are **info 0**, **notice 25**, **warning 50**, and **error 100**.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables VQM lost packet **info** messages to be logged if loss occurs above **10** packets:

(config)**#ip rtp quality-monitoring threshold loss info 10**

ip rtp quality-monitoring threshold lq-mos

Use the **ip rtp quality-monitoring threshold lq-mos** command to specify threshold values for logging listening quality (LQ) mean opinion score (MOS) events during voice quality monitoring (VQM). When the call quality detected in the Realtime Transport Protocol (RTP) stream is less than the specified event threshold, an event message is generated. Use the **no** form of this command disables the event reporting for that message type and threshold. Variations of this command include:

ip rtp quality-monitoring threshold lq-mos error
ip rtp quality-monitoring threshold lq-mos error <*value*>
ip rtp quality-monitoring threshold lq-mos info
ip rtp quality-monitoring threshold lq-mos info <*value*>
ip rtp quality-monitoring threshold lq-mos notice
ip rtp quality-monitoring threshold lq-mos notice <*value*>
ip rtp quality-monitoring threshold lq-mos warning
ip rtp quality-monitoring threshold lq-mos warning <*value*>

Syntax Description

error	Specifies the threshold for LQ MOS error messages to be logged.
info	Specifies the threshold for LQ MOS information messages to be logged.
notice	Specifies the threshold for LQ MOS notice messages to be logged.
warning	Specifies the threshold for LQ MOS warning messages to be logged.
<*value*>	Optional. The range is **0** to **4.4**.

Default Values

By default, the LQ MOS thresholds are **info 4.40**, **notice 4.00**, **warning 3.60**, and **error 2.60**.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables VQM LQ MOS **info** messages to be logged if LQ MOS scores fall below **4.25**:

(config)**#ip rtp quality-monitoring threshold lq-mos info 4.25**

ip rtp quality-monitoring threshold out-of-order

Use the **ip rtp quality-monitoring threshold out-of-order** command to specify threshold values for logging out-of-order packet events during voice quality monitoring (VQM). When more out-of-order packets are detected in the Realtime Transport Protocol (RTP) stream than the specified event threshold, an event message is generated. Use the **no** form of this command disables the event reporting for that message type and threshold. Variations of this command include:

ip rtp quality-monitoring threshold out-of-order error
ip rtp quality-monitoring threshold out-of-order error <*value*>
ip rtp quality-monitoring threshold out-of-order info
ip rtp quality-monitoring threshold out-of-order info <*value*>
ip rtp quality-monitoring threshold out-of-order notice
ip rtp quality-monitoring threshold out-of-order notice <*value*>
ip rtp quality-monitoring threshold out-of-order warning
ip rtp quality-monitoring threshold out-of-order warning <*value*>

Syntax Description

error	Specifies the threshold for out-of-order packet error messages to be logged.
info	Specifies the threshold for out-of-order packet information messages to be logged.
notice	Specifies the threshold for out-of-order packet notice messages to be logged.
warning	Specifies the threshold for out-of-order packet warning messages to be logged.
<*value*>	Optional. The range is **0** to **30000**.

Default Values

By default, the out-of-order packet thresholds are **info 0**, **notice 25**, **warning 50**, and **error 100**.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables VQM out-of-order packet **info** messages to be logged if the number of out-of-order packets is greater than **5**:

(config)**#ip rtp quality-monitoring threshold out-of-order info 5**

ip rtp quality-monitoring threshold pq-mos

Use the **ip rtp quality-monitoring threshold pq-mos** command to specify threshold values for logging perceived quality (PQ) mean opinion score (MOS) events during voice quality monitoring (VQM). When the call quality detected in the Realtime Transport Protocol (RTP) stream is less than the specified event threshold, an event message is generated. Use the **no** form of this command disables the event reporting for that message type and threshold. Variations of this command include:

ip rtp quality-monitoring threshold pq-mos error
ip rtp quality-monitoring threshold pq-mos error <*value*>
ip rtp quality-monitoring threshold pq-mos info
ip rtp quality-monitoring threshold pq-mos info <*value*>
ip rtp quality-monitoring threshold pq-mos notice
ip rtp quality-monitoring threshold pq-mos notice <*value*>
ip rtp quality-monitoring threshold pq-mos warning
ip rtp quality-monitoring threshold pq-mos warning <*value*>

Syntax Description

error	Specifies the threshold for listening quality PQ MOS error messages to be logged.
info	Specifies the threshold for listening quality PQ MOS information messages to be logged.
notice	Specifies the threshold for listening quality PQ MOS notice messages to be logged.
warning	Specifies the threshold for listening quality PQ MOS warning messages to be logged.
<*value*>	Optional. The range is **0** to **4.4**.

Default Values

By default, the PQ MOS thresholds are **info 4.40**, **notice 4.00**, **warning 3.60**, and **error 2.60**.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables VQM PQ MOS **info** messages to be logged if the PQ MOS scores fall below **4.25**:

(config)**#ip rtp quality-monitoring threshold pq-mos info 4.25**

ip rtp session timeout <*value*> disconnect

Use the **ip rtp session timeout** <*value*> **disconnect** command to specify the time, in seconds, before calls that have not received Realtime Transport Protocol (RTP) are disconnected. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the timeout period, in seconds, before disconnecting RTP calls once the RTP packet flow ends. Range is **32** to **900** seconds.

Default Values

By default, RTP sessions disconnect after **45** seconds of inactivity.

Command History

Release R13.8.0	Command was introduced.

Usage Examples

The following example specifies that after **60** seconds of no received RTP, RTP calls will be disconnected:

(config)**#ip rtp session timeout 60 disconnect**

ip rtp symmetric-filter

Use the **ip rtp symmetric-filter** command to enable filtering of received nonsymmetric Realtime Transport Protocol (RTP) packets. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the RTP symmetric filter is enabled on some AOS platforms, and disabled on others. Enter the **show running-config verbose | include rtp symmetric-filter** command from the Enable mode prompt to determine if the RTP symmetric filter is enabled or disabled on the AOS device.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example enables **ip rtp symmetric-filter**:

(config)**#ip rtp symmetric-filter**

ip rtp udp *<number>*

Use the **ip rtp udp** command to configure a global starting User Datagram Protocol (UDP) port for Realtime Transport Protocol (RTP). Use the **no** form of this command to remove a configured UDP port.

Syntax Description

<number>	Specifies the value of the starting UDP port. Valid range is **1026** to **60000**.

Default Values

The default value for this command is **10000**.

Command History

Release 10.1	Command was introduced.
Release 14.1	Command was updated.

Usage Examples

The following example configures **2000** as the starting value of the UDP port:

(config)**#ip rtp udp 2000**

ip scp server

Use the **ip scp server** command to enable the secure copy server functionality in AOS. Enabling the secure copy server allows AOS to support the transfer of files using a secure connection. A secure connection helps provide protection against outside forces gaining access to configuration files. An external secure copy server is required to facilitate the transfers from the terminal. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the secure copy server is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables the secure copy server function:

(config)**#ip scp server**

ip security monitor

Use the **ip security monitor** command to activate the AOS Security Monitor feature and enter the Security Monitor Configuration mode. For more information on configuring the Security Monitor feature, refer to the *Security Monitor Command Set on page 4503*.

Syntax Description

No Subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example activates the Security Monitor Configuration feature:

(config-)**#ip security monitor**

ip security monitor stats-filter <*name*>

Use the **ip security monitor stats-filter** command to create a new security monitor filter and enter the filter configuration mode. For more information on configuring the security monitor statistics filter refer to *threat on page 4506*. Use the **no** version of this command to delete the specified filter.

Syntax Description

<*name*>	Specifies the filter to be applied.

Default Values

By default, no security monitor filters exist.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example applies a filter named **F1**:

(config)**#ip security monitor stats-filter F1**
Creating new filter “F1”.
(config-secmon-filter)#

ip sntp server

Use the **ip sntp server** command to enable the Simple Network Time Protocol (SNTP) server. This allows the unit to accept SNTP requests. Use the **no** form of this command to disable the server.

Syntax Description

No subcommands.

Default Values

By default, the SNTP server is disabled.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example enables the SNTP server:

(config)**#ip sntp server**

ip sntp server send-unsynced

Use the **ip sntp server send-unsynced** command to enable sending the system clock time when requested, even if the device is not synchronized with the Simple Network Time Protocol (SNTP) server. Use the **no** form of this command to disable this setting.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example enables the device to send the system clock time regardless of synchronized status with the sntp server:

(config)**#ip sntp server send-unsynced**

ip sntp server source-interface <*interface*>

Use the **ip sntp server source-interface** command to specify a source interface for Simple Network Time Protocol (SNTP) server traffic. The IP address of the specified interface will be used to source all SNTP traffic. Use the **no** form of this command if you do not wish to override the default source IP address.

Syntax Description

<interface>	Specifies the source interface for SNTP server traffic. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip sntp server source-interface ?** for a complete list of valid interfaces.

Default Values

By default, no SNTP server source interface is defined.

Command History

Release 6.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 16.1	Command was expanded to include the bridged virtual interface (BVI), Frame Relay, high level data link control (HDLC), and Point-to-Point Protocol (PPP) interfaces.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for SNTP traffic:

(config)#**ip sntp server source-interface loopback 1**

ip sntp source-interface *<interface>*

Use the **ip sntp source-interface** command to specify a source interface for Simple Network Time Protocol (SNTP) traffic originated by the unit. The IP address of the specified interface will be used to source all SNTP traffic. Use the **no** form of this command if you do not wish to override the default source IP address.

Syntax Description

<interface>	Specifies the source interface for SNTP traffic. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip sntp source-interface ?** for a complete list of valid interfaces.

Default Values

By default, no SNTP source interface is defined.

Command History

Release 6.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 16.1	Command was expanded to include the bridged virtual interface (BVI), Frame Relay, high level data link control (HDLC), and Point-to-Point Protocol (PPP) interfaces.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for SNTP traffic:

(config)**#ip sntp source-interface loopback 1**

ip subnet-zero

The **ip subnet-zero** command is the default operation and cannot be disabled. This command signifies the router's ability to route to subnet-zero subnets.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example **subnet-zero** is enabled:

(config)**#ip subnet-zero**

ip tacacs source-interface <*interface*>

Use the **ip tacacs source-interface** command to specify an Internet Protocol version 4 (IPv4) source interface for terminal access controller access-control system plus (TACACS+) traffic originated by the unit. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the association to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the association to the default unnamed VRF. The IPv4 address of the specified interface will be used to source all TACACS+ traffic. Use the **no** form of this command if you do not wish to override the default source IP address. Variations of this command include:

ip tacacs source-interface <*interface*>
ip tacacs vrf <*name*> **source-interface** <*interface*>

Syntax Description

<*interface*>	Specifies the source interface for TACACS+ traffic. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip tacacs source-interface ?** for a complete list of valid interfaces.
vrf <*name*>	Specifies the name of the VRF to which to assign the source-interface.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for TACACS+ traffic:

(config)**#ip tacacs source-interface loopback 1**

The following example configures the unit to use the **loopback 1** interface on VRF RED as the source IP for TACACS+ traffic:

(config)**#ip tacacs vrf RED source-interface loopback 1**

ip urlfilter allowmode

Use the **ip urlfilter allowmode** command to allow all uniform resource locator (URL) requests in cases when all URL filter servers are down. Use the **no** form of this command to block all URL requests when all URL filter servers are down.

Syntax Description

No subcommands.

Default Values

By default, all URL requests will be blocked when all URL filter servers are down.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example permits all URL requests even when URL filter servers are down:

(config)**#ip urlfilter allowmode**

ip urlfilter exclusive-domain

Use the **ip urlfilter exclusive-domain** command to instruct AOS to always allow or always block a domain without first having to verify with the uniform resource locator (URL) filter server. Use the **no** form of this command to remove an exclusive domain. Variations of this command include:

ip urlfilter exclusive-domain deny *<name>*
ip urlfilter exclusive-domain permit *<name>*

Syntax Description

deny *<name>*	Specifies that the domain name be blocked without verifying with the URL filter server.
permit *<name>*	Specifies that the domain name be allowed without verifying with the URL filter server.

Default Values

By default, no exclusive domains are configured.

Command History

Release 12.1	Command was introduced.

Functional Notes

Domain matching is based on an exact match between the Hypertext Transfer Protocol (HTTP) header and entries in the **ip urlfilter exclusive-domain** command. In order to exactly match requests destined for a domain, entries should list all possible variations of the domain that would appear in the **Host** field of an HTTP header. Refer to the *Usage Examples* section of this command for more detailed information.

Usage Examples

The following example will always allow access to **www.adtran.com** and **adtran.com** without first having to verify the domain with the URL filter server:

(config)**#ip urlfilter exclusive-domain permit www.adtran.com**
(config)**#ip urlfilter exclusive-domain permit adtran.com**

The following example will always block access to **www.localnews.com** without first having to verify the domain with the URL filter server:

(config)**#ip urlfilter exclusive-domain deny www.localnews.com**

ip urlfilter <*name*> http

Use the **ip urlfilter http** command to create a uniform resource locator (URL) filter for Hypertext Transfer Protocol (HTTP) (Transmission Control Protocol (TCP) port 80) traffic. Use the **no** form of this command to delete the specified HTTP URL filter.

The URL filtering software runs on a server independent of the AOS product. For additional information about the URL filtering technology, refer to the vendor's website.

Syntax Description

<*name*>	Specifies the URL filter name.

Default Values

By default, no URL filters are configured.

Command History

Release 12.1	Command was introduced.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be applied to the appropriate interface by using the **ip urlfilter** <*name*> **[in | out]** command. Refer to this command in the appropriate interface for more information.

Usage Examples

The following example creates the HTTP URL filter called **MyFilter** that can be applied to an interface for content filtering:

(config)**#ip urlfilter MyFilter http**

ip urlfilter max-request <*value*>

Use the **ip urlfilter max-request** command to set the maximum number of outstanding uniform resource locator (URL) lookup requests that can be sent to a URL filter server without a response. Use the **no** form of this command to set the value back to its default setting.

Syntax Description

<*value*>	The maximum number of outstanding URL lookup requests. Valid range is **1** to **500** requests.

Default Values

By default, the number of outstanding requests is **500**.

Command History

Release 12.1	Command was introduced.

Functional Notes

After the maximum number of URL lookup requests is reached, the **no ip urlfilter allowmode** setting will be used to allow or block all following requests until enough URL lookup responses have been received from the URL filter server.

Usage Examples

The following example sets the maximum number of URL lookup requests to **250**:

(config)**#ip urlfilter max-request 250**

ip urlfilter max-response *<value>*

Use the **ip urlfilter max-response** command to set the maximum number of responses allowed to buffer before receiving an allow or block status from the uniform resource locator (URL) filter server. Use the **no** form of this command to set the value back to its default setting.

Syntax Description

<value>	Specifies the maximum number of responses allowed to buffer. Valid range is **1** to **100** responses.

Default Values

By default, the value of buffered responses is **100**.

Command History

Release 12.1	Command was introduced.

Functional Notes

When a URL request comes through the unit and URL filtering is enabled, a lookup request is sent to the URL filter server and the Hypertext Transfer Protocol (HTTP) request is forwarded to the HTTP server at the same time. If the HTTP server responds before the URL filter server, the response must be buffered until the URL filter server responds with **allow** or **block**. Once the maximum number of buffered HTTP responses is reached, all following HTTP responses are dropped until some of the existing buffered responses are released. Buffered responses are released when the URL filter server sends a response, or when the firewall association times out.

Usage Examples

The following example sets the maximum number of buffered responses to **50**:

(config)**#ip urlfilter max-response 50**

ip urlfilter server <*ip address*>

Use the **ip urlfilter server** command to identify a uniform resource locator (URL) filter server by IP address and port number. Use the **no** form of this command to remove the server from use. Variations of this command include:

ip urlfilter server <*ip address*>
ip urlfilter server <*ip address*> **port** <*number*>
ip urlfilter server <*ip address*> **timeout** <*value*>

Syntax Description

<*ip address*>	Specifies the server IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
port <*number*>	Specifies the server Transmission Control Protocol (TCP) port number that will receive requests.
timeout <*value*>	Specifies the number of seconds to wait for a response from the URL filtering server before determining that it is out of service. Range is **1** to **300** seconds.

Default Values

By default, there are no URL filtering servers configured. When configuring a URL filtering server, the port default is 15,868, and the timeout default is 5 seconds.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example identifies a URL filtering server at IP address **10.1.1.1** that listens for URL filtering requests on port 15,868 (default) and waits for a response for **10** seconds before determining that the filtering server is down:

(config)**#ip urlfilter server 10.1.1.1 timeout 10**

ip urlfilter top-website

Use the **ip urlfilter top-website** command to enable reporting of the websites most frequently requested on the system. Use the **no** form of this command to disable top websites reporting.

Enabling this feature may cause a performance degradation in Web browsing.

Syntax Description

No subcommands.

Default Values

By default, top websites reporting is disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables top websites reporting:

(config)**#ip urlfilter top-website**

ipv6 access-list extended *<ipv6 acl name>*

Use the **ipv6 access-list extended** command to create an empty Internet Protocol version 6 (IPv6) access control list (ACL) and enter the Extended ACL Configuration mode. Use the **no** form of this command to delete an extended ACL and all the entries contained in it.

> NOTE *For a complete list of all extended IPv6 ACL configuration commands, refer to the IPv4 Access Control List Command Set on page 4252.*

Syntax Description

<ipv6 acl name>	Specifies the name of the IPv6 ACL.

Default Values

By default, all AOS security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command only creates an empty extended IPv6 ACL, it does not configure it. For additional extended ACL configuration commands and configuration parameters, refer to the *IPv4 Access Control List Command Set on page 4252*.

Usage Examples

The following example creates an extended IPv6 ACL **Allowv6** and enters the Extended ACL Configuration mode:

(config)**#ip access-list extended Allowv6**
(config-ext6-nacl)#

Technology Review

IPv6 ACLs are used as packet selectors by different AOS IPv6 features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** ACL advances AOS to the next access policy entry. AOS provides two types of ACLs: standard and extended. Standard ACLs match based on the source of the packet. Extended ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

IPv6 ACLs cannot have the same name as IPv4 ACLs. If you are using both IPv4 and IPv6, you must have different ACLs for each IP version.

Virtual routing and forwarding (VRF) on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

ipv6 access-list standard *<ipv6 acl name>*

Use the **ipv6 access-list standard** command to create an empty IPv6 access control list (ACL) and enter the Standard ACL Configuration mode. Use the **no** form of this command to delete an extended ACL and all the entries contained in it.

For a complete list of all standard IPv6 ACL configuration commands, refer to the IPv6 Access Control Policy Command Set on page 4326.

Syntax Description

<ipv6 acl name>	Specifies the name of the IPv6 ACL.

Default Values

By default, all AOS security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command only creates an empty standard IPv6 ACL, it does not configure it. For additional standard IPv6 ACL configuration commands and configuration parameters, refer to the *IPv4 Access Control Policy Command Set on page 4278*.

Usage Examples

The following example creates a standard IPv6 ACL **Allowv6** and enters the Standard ACL Configuration mode:

(config)**#ipv6 access-list standard Allowv6**
(config-std6-nacl)#

Technology Review

IPv6 ACLs are used as packet selectors by different IPv6 AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** ACL advances AOS to the next access policy entry. AOS provides two types of ACLs: standard and extended. Standard ACLs match based on the source of the packet. Extended ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

IPv6 ACLs cannot have the same name as IPv4 ACLs. If you are using both IPv4 and IPv6, you must have different ACLs for each IP version.

Virtual routing and forwarding (VRF) on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

ipv6 crypto

Use the **ipv6 crypto** command to enable Internet Protocol version 6 (IPv6) IP security (IPsec). Use the **no** form of this command to disable IPv6 IPsec. Variations of this command include:

ipv6 crypto
ipv6 crypto vrf <*name*>

Syntax Description

vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to enable IPv6 IPsec. If no VRF is specified, IPv6 IPsec is enabled on the default unnamed VRF instance.

Default Values

By default, IPv6 IPsec is disabled.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example enables IPv6 IPsec on the default VRF instance:

(config)**#ipv6 crypto**

ipv6 crypto ipsec transform-set *<name> <parameters>*

Use the **ipv6 crypto ipsec transform-set** command to define an Internet Protocol version 6 (IPv6) transform set. Transform sets are used to define the configuration for securing data with IP security (IPsec), and then the sets are applied to crypto maps which use them for specific security algorithms. Use the **no** form of this command to remove the transform set.

The following additional subcommands are available once you have entered the Transform Set Configuration mode:

mode tunnel

Syntax Description

<name>	Specifies the name of the transform set. Names must be unique, and are specified in an alphanumeric string of up to **80** characters.	
<parameters>	Assigns a combination of up to three security algorithms to the set. Available security algorithms are as follows:	
	ah-md5-hmac	Authentication Header. Uses 16 byte key and HMAC-MD5-96 authentication.
	ah-sha-hmac	Authentication Header. Uses 20 byte key and HMAC-SHA1-96 authentication.
	esp-des	Encapsulating Security Payload. Data encryption standard using cipher block chaining and an 8-byte key (DES-56-CBC).
	esp-3des	Encapsulating Security Payload. Data encryption standard using cipher block chaining and a 24-byte key (3DES-168-CBC).
	esp-aes-128-cbc	Encapsulating Security Payload. Advanced encryption standard using cipher block chaining and a 16-byte key.
	esp-aes-192-cbc	Encapsulating Security Payload. Advanced encryption standard using cipher block chaining and a 24-byte key.
	esp-aes-256-cbc	Encapsulating Security Payload. Advanced encryption standard using cipher block chaining and a 32-byte key.
	esp-null	Encapsulating Security Payload with no encryption.
	esp-md5-hmac	Encapsulating Security Payload. Uses 16-byte key and HMAC-MD5-96 authentication.
	esp-sha-hmac	Encapsulating Security Payload. Uses 20-byte key and HMAC-SHA1-96 authentication.
mode tunnel	Specifies the encapsulation mode for the transform set is datagram encapsulation (tunnel) mode.	

Default Values

By default, no IPv6 IPsec transform sets are configured.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Transform sets are used to define the configuration for securing data with IPsec, and are then applied to crypto maps which reference them for specific security algorithms. Sets are applied using the command *set transform-set <name> on page 5259*. For manual key crypto maps, only one transform set can be specified. If no transform set is used in the crypto map, then the entry is incomplete and will have no effect on the system.

If the transform set is deleted, any references to the transform set by other functions are removed, leaving them incomplete.

Transform set names must be unique among IPv6 transform sets. Entering the name of an existing transform set re-enters the transform set configuration mode for that set.

Usage Examples

The following example creates the transform set **SET1** and its security algorithms:

(config)**#ipv6 crypto ipsec transform-set SET1 esp-3des esp-des**

ipv6 crypto map *<name> <index>*

Use the **ipv6 crypto map** command to create an Internet Protocol version 6 (IPv6) IP security (IPsec) crypto map entry and enter the crypto map entry's configuration mode. Use the **no** form of this command to remove the map and all it's settings. Variations of this command include:

ipv6 crypto map *<name> <index>*
ipv6 crypto map *<name> <index>* **ipsec-manual**

Syntax Description

<name>	Specifies the name of the IPv6 crypto map entry.
<index>	Specifies the crypto map entry sequence number. Valid range is **0** to **65535**.
ipsec-manual	Optional. Specifies that the map supports manually configured IPsec entries.

Default Values

By default, no IPv6 IPsec crypto maps exist.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

If the map is used on an interface, removing the map also removes the map on any interfaces to which it is assigned.

Usage Examples

The following example creates a manually-keyed IPv6 crypto map:

(config)**#ipv6 crypto map MAP1 10 ipsec-manual**

ipv6 crypto map <*name*> rpf-check

Use the **ipv6 crypto map rpf-check** command to enable the reverse path forwarding (RPF) check on the Internet Protocol version 6 (IPv6) IP security (IPsec) crypto map entry. This command enables checking of tunnel traffic to disallow tunnel traffic that is spoofed from another tunnel. The check is applied to any security association (SA) created from any entry in the named crypto map. Use the **no** form of this command to disable the RPF check.

Syntax Description

<*name*>	Specifies the crypto map on which to enable the RPF check.

Default Values

By default, RPF checks are enabled.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example enables RPF checking for crypto map **MAP1**:

(config)**#ipv6 crypto map MAP1 rpf-check**

ipv6 dhcp address client limit <*number*>

Use the **ipv6 dhcp address client limit** command to specify the maximum number of Internet Protocol version 6 (IPv6) addresses assigned per client by the Dynamic Host Control Protocol version 6 (DHCPv6) server. Use the **no** form of this command to return the maximum number of assigned addresses to the default value.

Syntax Description

<*number*>	Specifies the maximum number of IPv6 addresses that can be assigned to a single DHCPv6 client. Valid range is **0** to **500**. Setting the number to 0 returns the maximum number of allowed IPv6 addresses to the default value.

Default Values

By default, a maximum number of **50** IPv6 addresses can be assigned to a single DHCPv6 client.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example specifies the maximum number of IPv6 addresses that can be assigned to a single DHCPv6 client is **75**:

(config)**#ipv6 dhcp address client limit 75**

ipv6 dhcp address conflict limit <*number*>

Use the **ipv6 dhcp address conflict limit** command to specify the maximum number of conflicting Internet Protocol version 6 (IPv6) addresses that can be stored by the Dynamic Host Control Protocol version 6 (DHCPv6) server. This command limits the number of conflicting addresses stored by the DHCPv6 server to ensure that the AOS unit does not run out of memory. Use the **no** form of this command to reset the count to the default value.

Syntax Description

<*number*>	Specifies the maximum number of conflicting IPv6 addresses that can be stored by the server. Valid range is **1** to **10000** addresses. This maximum number is product-specific and is equivalent to the default value on the product.

Default Values

By default, only a certain number of conflicting IPv6 addresses can be stored. This number varies by AOS product.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example changes the number of conflicting IPv6 addresses stored by the DHCPv6 server to **3500:**

(config)**#ipv6 dhcp address conflict limit 3500**

ipv6 dhcp address limit *<number>*

Use the **ipv6 dhcp address limit** command to specify the maximum number of Internet Protocol version 6 (IPv6) addresses that can be assigned by the Dynamic Host Control Protocol version 6 (DHCPv6) server. This command limits the number of addresses assigned by the DHCPv6 server to ensure that the AOS unit does not run out of memory. Use the **no** form of this command to reset the count to the default value.

Syntax Description

<number>	Specifies the number of IPv6 addresses that can be assigned. Valid range is **1** to **10000**. This maximum number is product-specific, and is equivalent to the default value on the AOS unit.

Default Values

By default, only a certain number of addresses can be assigned by the DHCPv6 server. This number varies by AOS product.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example changes the maximum number of IPv6 addresses that can be assigned by the DHCPv6 server to **2000**:

(config)**#ipv6 dhcp address limit 2000**

ipv6 dhcp database local

Use the **ipv6 dhcp database local** command to enable the Dynamic Host Control Protocol version 6 (DHCPv6) database. The DHCPv6 database stores local DHCPv6 bindings, allowing Internet Protocol version 6 (IPv6) addresses assigned by the DHCPv6 server to be stored in non-volatile random access memory (NVRAM) and preserved across a reboot of the AOS unit. Using this command enables the local database to begin storing DHCPv6 information. Use the **no** form of this command to disable the DHCPv6 database.

Syntax Description

No subcommands.

Default Values

By default, the DHCPv6 database is disabled.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example enables the DHCPv6 database:

(config)**#ipv6 dhcp database local**

ipv6 dhcp excluded-address

Use the **ipv6 dhcp excluded-address** command to specify Internet Protocol version 6 (IPv6) addresses to exclude from any Dynamic Host Control Protocol version 6 (DHCPv6) server pool. These addresses are excluded from the DHCPv6 server pool, and cannot be assigned to DHCP clients by the server of these devices. Use the **no** form of this command to remove the address exclusion and make the address(es) available for use by the DHCPv6 server. Variations of this command include:

ipv6 dhcp excluded-address *<ipv6 address>*
ipv6 dhcp excluded-address *<beginning ipv6 address> <ending ipv6 address>*
ipv6 dhcp excluded-address vrf *<name> <ipv6 address>*
ipv6 dhcp excluded-address vrf *<name> <beginning ipv6 address> <ending ipv6 address>*

Syntax Description

<ipv6 address>	Specifies a single IPv6 address to exclude from any DHCPv6 server pool. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<beginning ipv6 address>	Specifies the lowest IPv6 address in the range of addresses to exclude. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<ending ipv6 address>	Specifies the highest IPv6 address in the range of addresses to exclude. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
vrf *<name>*	Optional. Specifies a nondefault named virtual routing and forwarding (VRF) instance on which to exclude the IPv6 addresses. If a VRF instance is not specified, the addresses are excluded on the default unnamed VRF instance.

Default Values

By default, no IPv6 addresses are excluded.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example excludes the IPv6 addresses on the default VRF instance ranging from **2001:DB8:1::1** to **2001:DB8:1::5** from any DHCPv6 server pool:

(config)**#ipv6 dhcp excluded-address 2001:DB8:1::1 2001:DB8:1::5**

ipv6 dhcp ping packets *<number>*

Use the **ipv6 dhcp ping packets** command to configure the number of ping packets transmitted by the Dynamic Host Control Protocol version 6 (DHCPv6) server when testing an Internet Protocol version 6 (IPv6) address before it is assigned to a client. Use the **no** form of this command to prevent the DHCPv6 server from using ping packets as part of the IPv6 address assignment process.

Syntax Description

<number>	Specifies the number of DHCPv6 ping packets sent on the network before assigning the IPv6 address to a requesting DHCPv6 client. Valid range is **0** to **100** packets.

Default Values

By default, **2** ping packets are sent to test IPv6 addresses before assigning them to a DHCPv6 client.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example specifies that **8** ping packets are used by DHCPv6 to test IPv6 addresses before assigning them to a client:

(config)**#ipv6 dhcp ping packets 8**

ipv6 dhcp ping timeout *<value>*

Use the **ipv6 dhcp ping timeout** command to specify the interval the Dynamic Host Control Protocol version 6 (DHCPv6) server waits for a response to a transmitted DHCPv6 ping packet when testing an Internet Protocol version 6 (IPv6) packet. Use the **no** form of this command to return the timeout period to the default value.

Syntax Description

<value>	Specifies the DHCPv6 ping timeout value in milliseconds. Valid range is **10** to **1000** ms.

Default Values

By default, the DHCPv6 server waits **500** ms for a ping response when testing an IPv6 address.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example specifies the ping timeout value for the DHCPv6 server is **300** ms:

(config)**#ipv6 dhcp ping timeout 300**

ipv6 dhcp pool <*name*>

Use the **ipv6 dhcp pool** command to create a Dynamic Host Control Protocol version 6 (DHCPv6) server address pool and enter the pool's configuration mode. The server pool is used to define the information to be assigned to DHCPv6 clients by the DHCPv6 server. The pool chosen to serve a specific client's request is determined by the current pool selection algorithm, just as in DHCP version 4 (DHCPv4). Use the **no** form of this command to remove the DHCPv6 server pool from the AOS unit's configuration. Refer to the *DHCPv6 Pool Command Set on page 4360* for more information.

Syntax Description

<*name*>	Specifies the name of the DHCPv6 pool using an alphanumeric string (up to 32 characters in length).

Default Values

By default, no DHCPv6 server pools are configured.

Command History

Release 18.3	Command was introduced.

Functional Notes

Use the **ipv6 dhcp pool** command to create multiple DHCPv6 server address pools for various segments of the network. Multiple address pools can be created to service different segments of the network with tailored configurations.

Usage Examples

The following example creates the DHCPv6 server address pool (labeled **Pool1**) and enters the DHCPv6 pool's configuration mode:

```
(config)#ipv6 dhcp pool Pool1
(config-dhcpv6)#
```


ipv6 dhcp prefix limit <*value*>

Use the **ipv6 dhcp prefix limit** command to limit the number of Internet Protocol version 6 (IPv6) prefixes that can be delegated by Dynamic Host Control Protocol (DHCPv6). Prefixes can be limited on a router or client basis. Use the **no** version of this command to remove the limit. Variations of this command include:

ipv6 dhcp prefix client limit <*value*>
ipv6 dhcp prefix limit <*value*>

Syntax Description

client	Optional. Limits the number of IPv6 prefixes that can be delegated to DHCPv6 clients.
<*value*>	Specifies the number of IPv6 prefixes that can be delegated. Valid range is **0** to **164352**. If the value is set to **0**, the limit is removed.

Default Values

By default, the IPv6 prefix limit for DHCPv6 is set to **0** (no limit).

Command History

Release R11.1.0	Command was introduced.

Usage Examples

The following example specifies a limit of **10** IPv6 prefixes for DHCPv6 clients:

(config)**#ipv6 dhcp prefix client limit 10**

ipv6 duplicate-address remove-route

Use the **ipv6 duplicate-address remove-route** command to specify that any duplicate IPv6 addresses detected by Duplicate Address Detection (DAD) are automatically removed from the IPv6 route table. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, any duplicate IPv6 addresses discovered by DAD remain in the IPv6 route table.

Command History

Release 13.6.0	Command was introduced.

Functional Notes

If this feature has been enabled, and then is disabled, a shutdown must be executed on the interfaces for which the duplicate IPv6 addresses should be retained. Without the shutdown, the duplicate address retention will not take effect.

Usage Examples

The following example specifies that duplicate IPv6 addresses detected by DAD are removed from the IPv6 route table:

(config)**#ipv6 duplicate-address remove-route**

ipv6 ffe limit exceptions *<value>*

Use the **ipv6 ffe limit exceptions** command to specify a limit to the number of unhandled Internet Protocol version 6 (IPv6) fast forwarding engine (FFE) exception packets allowed at any given time by the RapidRoute feature. Use the **no** form of this command to return the limit to the default value.

Syntax Description

<value>	Specifies the maximum number of unhandled FFE exception packets allowed at a given time. Valid range is **1** to **1024**.

Default Values

By default, no more than **128** exception packets are allowed.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

Exception packets are any packets that RapidRoute cannot handle, for example, traffic that matches ineligible entries, fragmented packets, packets with header errors, or the first packet in a given traffic flow that is used to build an FFE entry. Once the limit of unhandled FFE exception packets is reached, subsequent exception packets are dropped until the previously unhandled exceptions are resolved.

Usage Examples

The following example specifies the maximum number of IPv6 exception packets allowed by RapidRoute are **200**:

(config)**#ipv6 ffe limit exceptions 200**

ipv6 ffe max-entries <*value*>

Use the **ipv6 ffe max-entries** command to specify a global limit to the number of Internet Protocol version 6 (IPv6) fast forwarding engine (FFE) entries allowed at any given time by the RapidRoute feature. Use the **no** form of this command to return to the default value.

Issuing this command will cause all RapidRoute entries to be cleared from the unit.

Syntax Description

<*value*>	Specifies the total number of RapidRoute entries for all interfaces. Valid range is **1** to **500000**.

Default Values

By default, the **ipv6 ffe max-entries** is set to **16384**.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example sets the total maximum number of IPv6 RapidRoute entries to **500**:

(config)**#ipv6 ffe max-entries 500**

ipv6 ffe timeout

Use the **ipv6 ffe timeout** command to set the time to live (TTL) for Internet Protocol version 6 (IPv6) RapidRoute fast forwarding engine (FFE) entries based on their IPv6 protocol. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 ffe timeout ah <*max timeout*>
ipv6 ffe timeout ah <*max timeout*> <*inactive timeout*>
ipv6 ffe timeout esp <*max timeout*>
ipv6 ffe timeout esp <*max timeout*> <*inactive timeout*>
ipv6 ffe timeout gre <*max timeout*>
ipv6 ffe timeout gre <*max timeout*> <*inactive timeout*>
ipv6 ffe timeout icmp <*max timeout*>
ipv6 ffe timeout icmp <*max timeout*> <*inactive timeout*>
ipv6 ffe timeout other <*max timeout*>
ipv6 ffe timeout other <*max timeout*> <*inactive timeout*>
ipv6 ffe timeout tcp <*max timeout*>
ipv6 ffe timeout tcp <*max timeout*> <*inactive timeout*>
ipv6 ffe timeout udp <*max timeout*>
ipv6 ffe timeout udp <*max timeout*> <*inactive timeout*>

Syntax Description

ah	Specifies timeout values in seconds for Authentication Header (AH) Protocol.
esp	Specifies timeout values in seconds for Encapsulating Security Payload (ESP) Protocol.
gre	Specified timeout values in seconds for Generic Route Encapsulation (GRE) Protocol.
icmp	Specifies timeout values in seconds for Internet Control Message Protocol (ICMP).
other	Specifies timeout values in seconds for all protocols not listed.
tcp	Specifies timeout values in seconds for Transmission Control Protocol (TCP).
udp	Specifies timeout values in seconds for User Datagram Protocol (UDP).
<*max timeout*>	Specifies maximum age timeout in seconds. This is the maximum amount of time an entry will be kept in the RapidRoute table regardless of activity. Valid range is **60** to **86400** seconds.
<*inactive timeout*>	Optional. Specifies idle timeout in seconds. This is the amount of time an entry will remain in the RapidRoute table with no additional activity. Valid range is **10** to **86400** seconds.

Default Values

By default, the maximum age timeouts are set to **1800** seconds and the inactive timeouts are set to **15** seconds.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example sets the time to live for IPv6 RapidRoute entries of TCP packets to **1000** seconds.

(config)**#ipv6 ffe timeout tcp 1000**

ipv6 firewall

Use the **ipv6 firewall** command to enable AOS Internet Protocol version 6 (IPv6) security features, including IPv6 access control policies (ACPs) and lists (ACLs) and the stateful inspection firewall. Use the **no** form of this command to disable the IPv6 security functionality. Variations of this command include:

ipv6 firewall
ipv6 firewall vrf <*name*>

*Disabling the AOS IPv6 security features (using the **no ipv6 firewall** command) does not affect security configuration. All configuration parameters will remain intact, but no security data processing will be attempted.*

Syntax Description

vrf <*name*>	Optional. Enables or disables the IPv6 firewall for a specific virtual routing and forwarding (VRF) instance.

Default Values

By default, all AOS IPv6 security features are disabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example enables the AOS IPv6 security features:

(config)**#ipv6 firewall**

ipv6 firewall alg ftp

Use the **ipv6 firewall alg ftp** command to enable the Internet Protocol version 6 (IPv6) File Transfer Protocol (FTP) application-level gateway (ALG). Use the **no** form of this command to disable the FTP ALG. Variations of this command include:

ipv6 firewall alg ftp
ipv6 firewall alg ftp tcp
ipv6 firewall alg ftp tcp port <*port*>
ipv6 firewall vrf <*name*> **alg ftp**
ipv6 firewall vrf <*name*> **alg ftp tcp**
ipv6 firewall vrf <*name*> **alg ftp tcp port** <*port*>

Syntax Description

tcp	Optional. Specifies that the port on which the IPv6 FTP ALG is enabled is a Transmission Control Protocol (TCP) port.
port <*port*>	Optional. Specifies a single port on which to enable the IPv6 FTP ALG. Valid range is **0** to **65535**.
vrf <*name*>	Optional. Specifies a nondefault (named) Virtual Routing and Forwarding (VRF) instance on which to enable the IPv6 FTP ALG.

Default Values

By default, the IPv6 FTP ALG is enabled on all VRF instances on TCP port **21**.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The IPv6 FTP ALG operates by parsing the Layer 5 contents of packets used for FTP, and when necessary, opens pending policy sessions so that FTP data transfers are able to traverse the IPv6 firewall without being dropped by configured access control policies (ACPs). In addition, the IPv6 FTP ALG has the ability to perform FTP-specific attack checking.

During the process of an FTP flow, the IPv6 FTP ALG creates a pending policy session based on a currently active policy session. This pending policy session listens for expected FTP data transfer traffic.

Any IPv6 firewall policy sessions created using a stateless ACP entry bypass all ALG processing, even if the ALG is enabled for the ACP's destination port, allowing global ALG processing for specific ports, but bypassing the global configuration under certain circumstances (such as, on a particular ACP or for particular hosts or networks based on IPv6 ACLs).

The IPv6 FTP ALG cannot be enabled on a protocol and port that is the default protocol and port for any other ALG, even if the other ALG is disabled. The IPv6 FTP ALG also cannot be enabled on a TCP port whose default filtering behavior has been overridden.

Usage Examples

The following example disables the IPv6 FTP ALG on the default port (**21**), and then enables it on TCP ports **10000** and **20000** on the default VRF instance:

(config)**#no ipv6 firewall alg ftp tcp port 21**
(config)**#ipv6 firewall alg ftp tcp port 10000**
(config)**#ipv6 firewall alg ftp tcp port 20000**

ipv6 firewall attack-log threshold <*number*>

Use the **ipv6 firewall attack-log threshold** command to specify the number of possible attack conditions AOS will identify and block before generating a log message when using Internet Protocol version 6 (IPv6). Use the **no** form of this command to return to the default threshold. Variations of this command include:

ipv6 firewall attack-log threshold <*number*>
ipv6 firewall vrf <*name*> **attack-log threshold** <*number*>

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

<*number*>	Specifies the number of possible attack conditions AOS IPv6 will identify before generating a log message. Valid range is **0** to **4294967295**.
vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance to monitor. If no VRF is specified, the default unnamed VRF is monitored.

Default Values

By default, the **ipv6 firewall attack-log threshold** is set at **100**.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies a threshold of **25** attacks before generating a log message for the IPv6 firewall:

(config)**#ipv6 firewall attack-log threshold 25**

ipv6 firewall check duplicate-options

Use the **ipv6 firewall check duplicate-options** command to specify that Internet Protocol version 6 (IPv6) packets with duplicate options within a Destination Options or Hop-by-Hop Options extension headers are dropped. Using the **no** form of this command allows IPv6 packets with duplicate options. Variations of this command include:

ipv6 firewall check duplicate-options
ipv6 firewall vrf <*name*> **check duplicate-options**

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance on which to drop IPv6 packets with duplicate options headers. If no VRF is specified, the packets on the default unnamed VRF are dropped.

Default Values

By default, this feature is enabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that IPv6 packets with duplicate options headers are dropped on the default VRF:

(config)**#ipv6 firewall check duplicate-options**

ipv6 firewall check ftp-bounce

Use the **ipv6 firewall check ftp-bounce** command enable the File Transfer Protocol (FTP) bounce attack check for the Internet Protocol version 6 (IPv6) firewall. Use the **no** form of this command to disable the FTP bounce attack check. Variations of this command include:

ipv6 firewall check ftp-bounce
ipv6 firewall vrf <*name*> **check ftp-bounce**

Syntax Description

vrf <*name*>	Optional. Specifies a nondefault (named) Virtual Routing and Forwarding (VRF) instance on which the enable the bounce attack check. If no VRF instance is specified, the action is performed on the default unnamed VRF instance.

Default Values

By default, FTP bounce attack check is enabled on the IPv6 firewall.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

In addition to allowing the flow of IPv6 FTP traffic through the IPv6 firewall, the IPv6 FTP application-level gateway (ALG) can be used to protect against FTP bounce attacks. An FTP bounce attack is a network attack where malicious hosts using proxy FTP can target a specific well-known service on one server (Server A) by instructing another FTP server (Server B) to send a file to Server A that contains commands relevant to the service being attacked. For example, this can allow a malicious host to forge mail on Server A without making a direct connection. The lack of a direct file transfer between the attacker and the target server makes the identity of the attacker difficult to determine.

The IPv6 FTP ALG, however, can be used to protect against such an attack. When this feature is enabled, the IPv6 FTP ALG recognizes as an attack any extended port command (EPRT) sent by the FTP client that has a TCP port number less than **1024**, and the ALG closes the connection. The ALG performs this action because TCP port numbers in the range from **0** to **1023** are used by well-known services.

Although the IPv6 FTP ALG can perform bounce attack checks when ports less than 1024 are specified in an EPRT, services running on ports greater than 1023 are still vulnerable to FTP bounce attacks.

Usage Examples

The following example enables the FTP bounce attack check on the nondefault VRF instance **RED1**:

(config)**#ipv6 firewall vrf RED1 check ftp-bounce**

ipv6 firewall check header-order

Use the **ipv6 firewall check header-order** command to enable the dropping of Internet Protocol version 6 (IPv6) packets that have extension headers in an order different than the recommendations proposed in the Systems and Network Analysis Center (SNAC) document *Firewall Design Considerations for IPv6*. Use the **no** form of this command to disable the feature and allow the processing of IPv6 packets with extension headers according to RFC 2460. Variations of this command include:

ipv6 firewall check header-order

ipv6 firewall vrf <*name*> **check header-order**

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance to configure. If no VRF is specified, the default unnamed VRF is configured.

Default Values

By default, this feature is enabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that IPv6 packets with out-of-order headers are dropped on the default VRF:

(config)**#ipv6 firewall check header-order**

ipv6 firewall check min-fragment-size <*value*>

Use the **ipv6 firewall check min-fragment-size** command to specify the smallest permitted size for Internet Protocol version 6 (IPv6) fragmented packets. Packets less than the specified size are dropped. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 firewall check min-fragment-size <*value*>
ipv6 firewall vrf <*name*> **check min-fragment-size** <*value*>

> *The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.*

Syntax Description

<*value*>	Specifies the packet size in octets. Valid range is **56** to **1280** octets.
vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance to configure. If no VRF is specified, the default unnamed VRF is configured.

Default Values

By default, the IPv6 packet fragment size is set to **640** octets.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example changes the smallest permitted size for IPv6 packet fragments on the default VRF to **800** octets:

(config)**#ipv6 firewall check min-fragment-size 800**

ipv6 firewall check multiple-pad1

Use the **ipv6 firewall check multiple-pad1** command to specify that Internet Protocol version 6 (IPv6) packets with more than one Pad1 option back-to-back within the Destination Options or Hop-by-Hop Options extension headers are dropped. Use the **no** form of this command to allow packets with more than one Pad1 option back-to-back. Variations of this command include:

ipv6 firewall check multiple-pad1
ipv6 firewall vrf <*name*> **check multiple-pad1**

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance on which to drop IPv6 packets with multiple Pad1 options. If no VRF is specified, the packets on the default unnamed VRF are dropped.

Default Values

By default, this feature is disabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that packets on the default VRF with more than one Pad1 option are dropped:

(config)**#ipv6 firewall check multiple-pad1**

ipv6 firewall check reflexive-traffic

Use the **ipv6 firewall check reflexive-traffic** command to enable the AOS stateful inspection firewall to process Internet Protocol version 6 (IPv6) traffic and check for reflexive traffic. Reflexive traffic refers to packets that are routed out of the same interface on which they arrived. Use the **no** form of this command to disable this check. Variations of this command include:

ipv6 firewall check reflexive-traffic
ipv6 firewall vrf <*name*> **check reflexive-traffic**

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance on which to enable reflexive traffic checking. If no VRF is specified, IPv6 traffic is checked on the default unnamed VRF.

Default Values

By default, this reflexive traffic is allowed to bypass the firewall and does not create a policy session.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example enables the AOS IPv6 reflexive traffic check for the default VRF:

(config)**#ipv6 firewall check reflexive-traffic**

ipv6 firewall check tcp-seq-and-ack

Use the **ipv6 firewall check tcp-seq-and-ack** command to direct the Internet Protocol version 6 (IPv6) firewall to inspect each packet of a Transmission Control Protocol (TCP) flow to ensure that the sequence numbers and acknowledgement (ACK) numbers are within the expected window for that firewall session. Use the **no** form of this command to disable the TCP sequence and ACK number check. Variations of this command include:

ipv6 firewall check tcp-seq-and-ack
ipv6 firewall vrf <*name*> **check tcp-seq-and-ack**

Syntax Description

vrf <*name*>	Optional. Specifies a nondefault (named) Virtual Routing and Forwarding (VRF) instance on which to enable or disable the TCP sequence and ACK number check. If no VRF instance is specified, the action is performed on the default unnamed VRF instance.

Default Values

By default, the TCP sequence and ACK number check is enabled.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example enables the TCP sequence and ACK number check on the nondefault VRF instance **RED1**:

(config)**#ipv6 firewall vrf RED1 check tcp-seq-and-ack**

ipv6 firewall check udp-checksum-zero

Use the **ipv6 firewall check udp-checksum-zero** command to specify that Internet Protocol version 6 (IPv6) User Datagram Protocol (UDP) packets with a checksum value of zero are dropped. Use the **no** form of this command to allow UDP packets with a checksum value of zero. Variations of this command include:

ipv6 firewall check udp-checksum-zero

ipv6 firewall vrf <*name*> **check udp-checksum-zero**

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Descriptions

vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance on which to check UDP packets. If no VRF is specified, the default unnamed VRF is inspected.

Default Values

By default, this feature is enabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that UDP packets with a value of zero are dropped on the default VRF:

(config)**#ipv6 firewall check udp-checksum-zero**

ipv6 firewall check unknown-options

Use the **ipv6 firewall check unknown-options** command to specify that Internet Protocol version 6 (IPv6) packets with unknown options in the Destination Options or Hop-by-Hop Options extension headers are dropped. Use the **no** form of this command to allow IPv6 packets with unknown options in the extension header. Variations of this command include:

ipv6 firewall check unknown-options
ipv6 firewall vrf <*name*> **check unknown-options**

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance on which to check IPv6 packets. If no VRF is specified, traffic on the default unnamed VRF is dropped.

Default Values

By default, this feature is enabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that IPv6 packets with unknown option extension headers are dropped on the default VRF:

(config)**#ipv6 firewall check unknown-options**

ipv6 firewall fast-allow-failover

Use the **ipv6 firewall fast-allow-failover** command to automatically clear all open Internet Protocol version 6 (IPv6) firewall policy allow sessions when a route table change occurs. This allows the router to immediately send traffic to the failover interface. Use the **no** form of this command to disable this feature.Vairations of this command include:

ipv6 firewall fast-allow-failover
ipv6 firewall vrf <*name*> **fast-allow-failover**

> NOTE *The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.*

Syntax Description

vrf <*name*>	Optional. Enables or disables fast allow failover on the IPv6 firewall for a specific virtual routing and forwarding (VRF) instance.

Default Values

By default, all AOS IPv6 security features are disabled until the IPv6 firewall is enabled. By default, **fast-allow-failover** is disabled.

Command History

Release R10.4.0	Command was introduced.

Functional Note

If the command is not enabled, the router tries to send traffic from existing allowed policy sessions out from the failed IPv6 address until the session times out, resulting in a loss of connectivity. This command should be configured when destination-specific rules are configured. Destination-specific rules are most often used in failover and IPv6 load sharing configurations. Refer to the command *ipv6 policy-class <ipv6 acp name> on page 1549* for more information.

Usage Examples

The following example enables **fast-allow-failover**:

(config)**#ipv6 firewall fast-allow-failover**

ipv6 firewall filtering-behavior

Use the **ipv6 firewall filtering-behavior** command to modify the filtering behavior of the Internet Protocol version 6 (IPv6) firewall. Modifying the filtering behavior settings for a particular port and protocol allow for application-level gateway (ALG)-like behavior in certain applications without requiring parsing of the Layer 5 packet contents used by these applications. By modifying IPv6 firewall filtering behavior, you can enable firewall traversal for applications by adding one or more configuration options if no ALG is available for the application (such as with Trivial File Transfer Protocol (TFTP)). Use the **no** form of this command to return the firewall filtering behavior to the default value. Variations of this command include:

ipv6 firewall filtering-behavior [tcp <*port*> **| udp** <*port*>**] address-dependent**
ipv6 firewall filtering-behavior [tcp <*port*> **| udp** <*port*>**] address-port-dependent**
ipv6 firewall filtering-behavior [tcp <*port*> **| udp** <*port*>**] endpoint-independent**
ipv6 firewall vrf <*name*> **filtering-behavior [tcp** <*port*> **| udp** <*port*>**] address-dependent**
ipv6 firewall vrf <*name*> **filtering-behavior [tcp** <*port*> **| udp** <*port*>**] address-port-dependent**
ipv6 firewall vrf <*name*> **filtering-behavior [tcp** <*port*> **| udp** <*port*>**] endpoint-independent**

Syntax Description

tcp <*port*>	Specifies a Transmission Control Protocol (TCP) port for which the IPv6 firewall filtering behavior is changed. Valid range is **0** to **65535**. The port corresponds to the destination port of the firewall policy session, which is the destination port of the internal traffic.
udp <*port*>	Specifies a User Datagram Protocol (UDP) port for which the IPv6 firewall filtering behavior is changed. Valid range is **0** to **65535**. The port corresponds to the destination port of the firewall policy session, which is the destination port of the internal traffic.
address-dependent	Specifies that address-dependent filtering is used for traffic initiated using the specified destination port.
address-port-dependent	Specifies that address- and port-dependent filtering is used for traffic initiated using the specified destination port. This is the default firewall filtering behavior for most ports.
endpoint-independent	Specifies that endpoint-independent filtering is used for traffic initiated using the specified destination port.
vrf <*name*>	Optional. Specifies a nondefault (named) Virtual Routing and Forwarding (VRF) instance on which to apply the filtering behavior. If no VRF instance is specified, the action is performed on the default unnamed VRF instance.

Default Values

By default, most ports are filtered by traditional firewall filtering (**address-port-dependent**). By default, UDP port **69**, the TFTP port, uses **address-dependent** filtering.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

In AOS firmware release R10.1.0, the ability to configure IPv6 firewall filtering behavior was introduced. The ordinary filtering behavior of the IPv6 firewall is to restrict permitted return traffic to the exact source and destination IP addresses and ports of the initial traffic flow. This is called address- and port-dependent filtering. In some applications, including TFTP, the external traffic generated as part of the application can respond from a different external port than the one specified in the firewall configuration. This traffic might not be allowed to traverse the firewall, depending on the configured access control policy (ACP) rules. If available, an ALG could be used to accommodate such an application. The ALG would parse the application layer payload for traffic from the initiating host, and create an appropriate pending policy session to allow the expected response. With the release of R10.1.0, the IPv6 firewall incorporates two additional configurable filtering behaviors that can take the place of such ALGs for certain applications.

The first additional method of firewall filtering is using **address-dependent** filtering. In this type of filtering, return traffic from an external host to the initiating internal host is allowed from any port, but traffic originating from any other external host will continue to be blocked. The second additional method of firewall filtering is using **endpoint-independent** filtering. In this type of filtering, any external host can respond to traffic from the initiating host from any port.

For more information about the configuration and use of IPv6 firewall filtering behaviors, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that on the default unnamed VRF instance, TCP port **10000** and UDP port **40** are filtered by **endpoint-independent** filtering and that TCP port **20000** and UDP port **30** are filtered by **address-dependent** filtering:

(config)**#ipv6 firewall filtering-behavior tcp 10000 endpoint-independent**
(config)**#ipv6 firewall filtering-behavior tcp 20000 address-dependent**
(config)**#ipv6 firewall filtering-behavior udp 30 address-dependent**
(config)**#ipv6 firewall filtering-behavior udp 40 endpoint-independent**

ipv6 firewall fin-timeout <*timeout*>

Use the **ipv6 firewall fin-timeout** command to configure the firewall policy session timeout for a Transmission Control Protocol (TCP) policy session closed by a bidirectional FINISH (FIN). The policy session timeout determines when the time to live (TTL) for the session expires, and thus ends the session. Using the **no** form of this command returns the timeout to the default value. Variations of this command include:

ipv6 firewall fin-timeout <*timeout*>
ipv6 firewall vrf <*name*> **fin-timeout** <*timeout*>

Syntax Description

<*timeout*>	Specifies the session timeout in seconds. Valid range is **0** to **4294967295** seconds.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to perform the timeout. If no VRF is specified, the action occurs on the default unnamed VRF.

Default Values

By default, the FIN timeout is set to **4** seconds.

Command History

Release 18.2	Command was introduced.

Functional Notes

A policy session closed by a TCP FIN is one in which a FIN has been received from both endpoints participating in the session. This command is used when configuring firewall session timeouts for Internet Protocol version 6 (IPv6).

If the timeout is defined to be zero, the policy session will be deleted immediately without entering a post-connection state. This could be necessary for hosts that do not implement the TIME_WAIT TCP state correctly, but instead permit immediately reopening closed sessions.

Usage Examples

The following example changes the IPv6 firewall session timeout for TCP policy sessions closed by a FIN to **10** seconds:

(config)**#ipv6 firewall fin-timeout 10**

ipv6 firewall local-traffic-only

Use the **ipv6 firewall local-traffic-only** command to enable the Internet Protocol version 6 (IPv6) firewall for the processing of local traffic only. Forwarded traffic is not sent to the firewall when this feature is enabled. Use the **no** form of this command to disable the IPv6 firewall. Variations of this command include:

ipv6 firewall local-traffic-only
ipv6 firewall vrf <*name*> **local-traffic-only**

Syntax Description

vrf <*name*>	Optional. Specifies that the local traffic firewall is enabled on the specified virtual routing and forwarding (VRF) instance. If no VRF is specified, the firewall is enabled on the default (unnamed) VRF.

Default Values

By default, the IPv6 firewall is disabled.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

When the firewall is configured to process local traffic only (traffic arriving at the unit's local IP stack), routed traffic is allowed to flow through the AOS unit uninspected, but locally destined traffic is inspected by the firewall. This feature allows the firewall to protect local services running on the AOS unit even when routed traffic bypasses the firewall. When local traffic processing is enabled, several other security features are impacted, such as IPsec, policy classes, IP route cache, and Generic Routing Encapsulation (GRE).

- Local traffic only firewall processing cannot be used with cryptography (**ipv6 crypto**) because for IPsec to function, traffic must proceed through the firewall. If the firewall is configured to process local traffic only, routed traffic that requires IPsec protection will not flow through the firewall and therefore will not receive IPsec protection.
- Policy classes are applied only to traffic destined to the local stack when local traffic processing is enabled. The **self** policy class is applied to local traffic originating from the local stack, allowing all traffic, and cannot be changed.
- IP route cache entries are not created for local destinations or for the Loopback interface when local traffic processing enabled.
- Local GRE traffic encapsulated by a GRE tunnel interface will bypass the firewall when local traffic processing is enabled.
-

For additional IPv6 firewall configuration information, refer to *ipv6 firewall on page 1523*.

Usage Examples

The following example enables the firewall for local traffic processing on the default VRF:

(config)**#ipv6 firewall local-traffic-only**

ipv6 firewall policy-log threshold <*value*>

Use the **ipv6 firewall policy-log threshold** command to specify the number of Internet Protocol version 6 (IPv6) access control policy (ACP) events identified by AOS before generating a log message. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 firewall policy-log threshold <*value*>
ipv6 firewall vrf <*name*> **policy-log threshold** <*value*>

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

<*value*>	Specifies the number of IPv6 policy events AOS identifies before creating the log. Valid range is **1** to **4294967295**.
vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance for AOS to monitor. If no VRF is specified, the default unnamed VRF is monitored.

Default Values

By default, a log is generated after **100** policy events have been identified.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that a log is generated when **150** IPv6 ACP events are detected on the default VRF:

(config)**#ipv6 firewall policy-log threshold 150**

ipv6 firewall rst-timeout <*timeout*>

Use the **ipv6 firewall rst-timeout** command to configure the firewall policy session timeout for a Transmission Control Protocol (TCP) policy session closed by a RESET (RST). The policy session timeout determines when the time to live (TTL) for the session expires, and thus ends the session. Using the **no** form of this command returns the timeout to the default value. Variations of this command include:

ipv6 firewall rst-timeout <*timeout*>
ipv6 firewall vrf <*name*> **rst-timeout** <*timeout*>

Syntax Description

<*timeout*>	Specifies the session timeout in seconds. Valid range is **0** to **4294967295** seconds.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to perform the timeout. If no VRF is specified, the action occurs on the default unnamed VRF.

Default Values

By default, the RST timeout is set to **20** seconds.

Command History

Release 18.2	Command was introduced.

Functional Notes

A TCP policy session closed by an RST is one in which an RST has been received from both endpoints participating in the session, indicating that enough time has passed to complete the TCP reset process. This command is used when configuring firewall session timeouts for Internet Protocol version 6 (IPv6).

If the timeout is defined to be zero, the policy session will be deleted immediately without entering a post-connection state. This could be necessary for hosts that do not implement the TIME_WAIT TCP state correctly, but instead permit immediately reopening closed sessions.

Usage Examples

The following example changes the IPv6 firewall session timeout for TCP policy sessions closed by a RST sessions to **30** seconds:

(config)**#ipv6 firewall rst-timeout 30**

ipv6 firewall stealth

Use the **ipv6 firewall stealth** command to place the Internet Protocol version 6 (IPv6) firewall in stealth mode. The stealth setting allows the route to be invisible as a route hop to associated devices. Use the **no** form of this command to disable the stealth feature. Variations of this command include:

ipv6 firewall stealth
ipv6 firewall vrf <*name*> **stealth**

The AOS IPv6 firewall must be enabled (using the command ipv6 firewall on page 1523) for the stateful inspection firewall to be activated.

Syntax Description

vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance to put in stealth mode. If no VRF is specified, the default unnamed VRF is placed in stealth mode.

Default Values

By default, stealth mode is disabled.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example enables the **stealth** option for the default IPv6 VRF:

(config)**#ipv6 firewall stealth**

ipv6 firewall tcp-unestab-timeout <*timeout*>

Use the **ipv6 firewall tcp-unestab-timeout** command to configure the firewall policy session timeout for a pre-established Transmission Control Protocol (TCP) policy session. The policy session timeout determines when the time to live (TTL) for the session expires, and thus ends the session. Using the **no** form of this command returns the timeout to the default value. Variations of this command include:

ipv6 firewall tcp-unestab-timeout <*timeout*>
ipv6 firewall vrf <*name*> **tcp-unestab-timeout** <*timeout*>

Syntax Description

<*timeout*>	Specifies the session timeout in seconds. Valid range is **0** to **4294967295** seconds.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to perform the timeout. If no VRF is specified, the action occurs on the default unnamed VRF.

Default Values

By default, the timeout is set to **20** seconds for pre-established TCP firewall sessions.

Command History

Release 18.2	Command was introduced.

Functional Notes

A pre-established TCP policy session is a firewall session that has been opened by a TCP SYN, on which the full three-way TCP handshake has not yet been observed. This command is used when configuring firewall session timeouts for Internet Protocol version 6 (IPv6), and specifies the time period allowed for TCP to complete the three-way handshake at the beginning of the connection.

Usage Examples

The following example changes the IPv6 firewall session timeout for pre-established TCP sessions to **30** seconds:

(config)**#ipv6 firewall tcp-unestab-timeout 30**

ipv6 load-sharing

Use the **ipv6 load-sharing** command to allow parallel routes in the Internet Protocol version 6 (IPv6) route table to be used to balance IPv6 traffic to a specific destination across up to six equal paths. When this command is enabled, the IPv6 route table can use multiple *best* routes and alternate between them. When this command is disabled, the IPv6 route table uses a single *best* route. Use the **no** form of this command to disable IPv6 load sharing. Variations of this command include:

ipv6 load-sharing per-destination
ipv6 load-sharing per-packet

Syntax Description

per-destination	Specifies that the route used to forward a packet is based on a hash of the source and destination IPv6 packet.
per-packet	Specifies that each forwarding route lookup rotates through all the parallel *best* routes.

Default Values

By default, IPv6 load sharing is disabled.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example enables IPv6 load sharing based on the source and destination of the IPv6 packets:

(config)**#ipv6 load-sharing per-destination**

ipv6 named-prefix *<prefix name> <ipv6 prefix/prefix-length>*

Use the **ipv6 named-prefix** command to manually assign a value to a named Internet Protocol version 6 (IPv6) prefix. A named prefix is useful when the upper part of the prefix could change over time (such as when using provider-dependent addresses in Dynamic Host Control Protocol for IPv6 (DHCPv6)). By creating a named prefix, the variable holding the value of the prefix is defined once, and then applied in various ways without having to manually enter the prefix value at each use. Use the **no** form of this command to remove one prefix from within a named prefix when the prefix and prefix length are specified, or to remove all prefixes from within a named prefix if entered with only the prefix name. Variations of this command include:

ipv6 named-prefix *<prefix name> <ipv6 prefix/prefix-length>*
ipv6 named-prefix *<prefix name> <ipv6 prefix/prefix-length>* **expiration-date** *<date> <time>*

Syntax Description

<prefix name>	Specifies the name of the variable that holds the service provider assigned value for the prefix.
<ipv6 prefix/prefix-length>	Specifies the numerical value and length of the prefix. The prefix value is specified in colon hexadecimal format (**X:X::X/<Z>**), for example: **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**. The IPv6 prefix cannot be a link-local address.
expiration-date *<date> <time>*	Optional. Specifies the time at which the prefix will expire. Enter future expiration date value in the MM/DD/YY format, and the time parameter in the HH:MM or HH:MM:SS format.

Default Values

By default, no named prefixes exist.

Command History

Release R10.9.0	Command was introduced.

Functional Notes

Changes made to the named prefix are automatically applied at each interface using the named prefix form of the IPv6 address command.

Usage Examples

The following example assigns a value to the previously created prefix **PREFIX1**:

(config)**#ipv6 named-prefix PREFIX1 2001:DB8:3F::/64**

ipv6 neighbor *<ipv6 address> <interface> <mac address>*

Use the **ipv6 neighbor** command to manually enter a static entry into the Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) cache. Use the **no** form of this command to remove the static entry from the neighbor cache. Variations of this command include:

ipv6 neighbor *<ipv6 address> <interface> <mac address>*
ipv6 neighbor *<ipv6 address>* **mef-ethernet** *<slot/port> <mac address>*
ipv6 neighbor *<ipv6 address>* **system-control-evc**
ipv6 neighbor *<ipv6 address>* **system-control-evc** *<mac address>*
ipv6 neighbor *<ipv6 address>* **system-management-evc**
ipv6 neighbor *<ipv6 address>* **system-management-evc** *<mac address>*

Syntax Description

<ipv6 address>	Specifies the IPv6 address of the neighbor entry. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<interface>	Specifies the interface of the link on which the neighbor entry is connected. Interfaces are specified using the *<interface> <slot/port* | *interface id>* format. For example, to specify a Point-to-Point Protocol (PPP) interface, enter **ppp 1**.
<mac address>	Specifies the medium access control (MAC) address of the neighbor. MAC addresses should be expressed in the following format: XX:XX:XX:XX:XX:XX (for example, **00:A0:C8:00:00:01**).
mef-ethernet *<slot/port>*	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC exists by default and cannot be deleted.
system-management-evc	Specifies the system management EVC. This EVC exists by default and cannot be deleted.

Default Values

By default, no static neighbor entries exist in the neighbor cache.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was changed to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

In IPv6, neighbors are usually managed dynamically using the ND protocol. However, you can manually enter a static entry into the neighbor cache using the **ipv6 neighbor** command. When you enter a static entry into the neighbor cache, you should be aware of the following:

- A static entry entirely overrides an existing or new dynamic entry learned through ND.
- Neighbor unreachability detection (NUD) is not performed on static neighbors, so the neighbor's state is limited to either an incomplete modified state (interface is down) or a reachable modified state (interface is up).
- Using the **no** form of the **ipv6 neighbor** command removes static entries and not dynamic entries from the neighbor cache.
- Using the command *clear ipv6 neighbors on page 172* clears the dynamic entries from the neighbor cache, but not the static entries.
- Disabling IPv6 on an interface does not remove the static neighbor cache entries, although it will change the entry state to incomplete.

Usage Examples

The following example adds a static neighbor with an IPv6 address of **2001:DB8:3F::/48** on the Ethernet 0/1 interface, and has a MAC address of **00:A0:C8:00:00:01** to the neighbor cache:

(config)**#ipv6 neighbor 2001:DB8:3F::/48 ethernet 0/1 00:A0:C8:00:00:01**

ipv6 policy-class *<ipv6 acp name>*

Use the **ipv6 policy-class** command to create an Internet Protocol version 6 (IPv6) access control policy (ACP) and enter the ACP configuration mode. Use the **no** form of this command to delete an IPv6 ACP and all the entries it contains. Each ACP can contain up to 20 entries. For more information, refer to the *IPv6 Access Control Policy Command Set on page 4326*.

Configured IPv6 ACPs will only be active if the command ipv6 firewall on page 1523 has been entered at the Global Configuration mode prompt to enable the AOS IPv6 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.

Before applying an ACP to an interface, verify your Telnet or secure shell (SSH) connection will not be affected by the policy. If an ACP is applied to the interface you are connecting through and it does not allow Telnet or SSH traffic, your connection will be lost.

Syntax Description

<ipv6 acp name>	Identifies the configured IPv6 ACP using an alphanumeric descriptor (maximum of 50 characters). All ACP descriptors are case sensitive.

Default Values

By default, there are no configured IPv6 ACPs.

Command History

Release 18.1	Command was introduced.

Functional Notes

AOS IPv6 ACPs are used to allow or discard data for each physical interface. Each IPv6 ACP consists of an action (**allow**, **discard**) and a selector IPv6 access control list (ACL). When IPv6 packets are received on an interface, the configured IPv6 ACPs are applied to determine whether the data will be processed or discarded.

IPv6 ACPs only work with IPv6 ACLs, and IPv4 ACPs only work with IPv4 ACLs. You cannot have an IPv6 ACP or ACL with the same name as an IPv4 ACP or ACL.

Usage Examples

The following example creates an IPv6 ACP named **PRIVATEv6**:

```
(config)#ip policy-class PRIVATEv6
(config-policy6-class)#
```

ipv6 policy-class *<ipv6 acp name>* max-sessions *<number>*

Use the **ipv6 policy-class max-sessions** command to specify the maximum number of allowed Internet Protocol version 6 (IPv6) policy sessions on a specific IPv6 access control policy (ACP). For more details on IPv6 ACP functionality in AOS, refer to the *IPv6 Access Control Policy Command Set on page 4326*. Use the **no** form of this command to return to the default value.

Syntax Description

<ipv6 acp name>	Identifies the configured IPv6 ACP to which the maximum session limit is applied. Use an alphanumeric descriptor (maximum of 50 characters). All ACP descriptors are case sensitive.
<number>	Specifies the maximum number of allowed IPv6 ACP sessions. Valid range is **1** up to a value based on the amount of RAM in the AOS unit (refer to *Default Values* below).

Default Values

By default, the maximum IPv6 ACP sessions allowed are based on the amount of RAM in the AOS unit. The following table outlines the default values based on RAM:

RAM Amount	Default Max Sessions
64 MB	10000
128 MB	30000
256 MB	80000
512 MB	200000
768 MB	300000
1 GB	450000

Command History

Release 18.1	Command was introduced.

Functional Notes

To set the system-wide maximum limit for ACP sessions (both IPv4 and IPv6), use the command *policy-class max-sessions <number> on page 1654*.

Usage Examples

The following example allows no more than **100** policy sessions on the IPv6 ACP named **PRIVATEv6**:

(config)**#ipv6 policy-class PRIVATEv6 max-sessions 100**

ipv6 policy-class *<ipv6 acp name>* rpf-check

Use the **ipv6 policy-class rpf-check** command to verify that Internet Protocol version 6 (IPv6) traffic has entered on the appropriate interface using a route lookup. Reverse path forwarding (RPF) is essentially a spoofing check. For more details on IPv6 policy class functionality in AOS, refer to the *IPv6 Access Control Policy Command Set on page 4326*. Use the **no** form of this command to disable this feature.

Syntax Description

<ipv6 acp name>	Identifies the configured IPv6 access control policy (ACP) using an alphanumeric descriptor (maximum of 50 characters). All ACP descriptors are case sensitive.
rpf-check	Enables RPF check (spoofing).

Default Values

This command is enabled by default.

Command History

Release 18.1	Command was introduced.

Functional Notes

When enabled, after an IPv6 packet is received, the IPv6 firewall performs a route lookup on the packet's source IPv6 address to determine what interface would be used to forward the packet back to that address. The firewall then checks the IPv6 ACP assigned to that interface. If the IPv6 ACP does not match the IPv6 ACP of the interface on which the packet was received, the packet is dropped.

The **rpf-check** feature should be disabled if your application allows traffic to arrive on an interface sourced from networks contradicting the route table. This feature can be disabled on a per ACP basis by issuing this command in conjunction with the ACP name you do not want to be checked.

Usage Examples

The following example turns off the **rpf-check** feature for the IPv6 ACP named **PRIVATEv6**:

(config)**#no ip policy-class PRIVATEv6 rpf-check**

ipv6 policy-timeout

Use multiple **ipv6 policy-timeout** commands to customize policy timeout intervals for established Internet Protocol version 6 (IPv6) firewall sessions. The policy session timeout determines when the time to live (TTL) for the session expires and ends the session. This command configures the policy timeout for the following protocols: (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol version 6 (ICMPv6), Authentication Header (AH) Protocol, generic routing encapsulation (GRE), encapsulating security payload (ESP)) or specific services (by listing the particular port number). Use the **no** form of this command to return to the default timeout values. Variations of this command include:

ipv6 policy-timeout [vrf <*name*>**] match** <*ipv6 acl name*> **[policy** <*ipv6 acp name*>**]** <*timeout*>
ipv6 policy-timeout [vrf <*name*>**] [all-protocols | ahp | esp | gre | icmpv6 | tcp | udp |** <*protocol number*>**] [policy** <*ipv6 acp name*>**]** <*timeout*>
ipv6 policy-timeout [vrf <*name*>**] [tcp | udp] all-ports [policy** <*ipv6 acp name*>**]** <*timeout*>
ipv6 policy-timeout [vrf <*name*>**] [tcp | udp]** <*port*> **[policy** <*ipv6 acp name*>**]** <*timeout*>
ipv6 policy-timeout [vrf <*name*>**] [tcp | udp] range** <*beginning port*> <*ending port*> **[policy** <*ipv6 acp name*>**]** <*timeout*>

Syntax Description

<*timeout*>	Specifies the wait interval (in seconds) before an active session is closed. Valid range is **1** to **4294967295** seconds.
match <*ipv6 acl name*>	Specifies that if traffic creating the policy session matches the specified IPv6 access control list (ACL), the policy timeout value set using this command is used for the policy session. Because an ACL can be used to specify protocol and port information, you do not need to specify ports or protocols when using this version of the command. If the named ACL does not exist when this command is issued, an implicit ACL is created.
policy <*ipv6 acp name*>	Optional. Specifies that if the policy session uses the specified IPv6 access control policy (ACP) as its ingress policy class, the policy timeout value set using this command is used for the policy session (provided the ACL or protocol/port information matches if specified). If the named ACP does not exist when this command is issued, an implicit ACP is created.
ahp	Specifies the data protocol as AHP.
esp	Specifies the data protocol as ESP.
gre	Specifies the data protocol as GRE.
icmpv6	Specifies the data protocol as ICMPv6.
all-protocols	Specifies the timeout for all protocols. This policy session timeout is used when a specific protocol match is not found.

<protocol number>	Specifies the IPv6 next header value (protocol number) to match for using the specified timeout. Valid protocol number range is **0** to **255**. The following are accepted protocol numbers and their associated protocols: **51** (AHP), **50** (ESP), **47** (GRE), **58** (ICMPv6), **6** (TCP), and **17** (UDP). Protocol numbers reserved for extension headers cannot be used. For example, you cannot use **0** (hop-by-hop options), **43** (routing), **44** (fragment), **59** (no next header), **60** (destination options), or **135** (mobility).
tcp	Specifies the data protocol as TCP. If you are using TCP, you can also specify the timeout for a specific port, a range of ports, or all TCP ports.
udp	Specifies the data protocol as UDP. If you are using UDP, you can also specify the timeout for a specific port, a range of ports, or all UDP ports.
all-ports	Specifies all ports of either TCP or UDP are used if a specific match is not found.
<port>	Specifies a single TCP or UDP port. Keywords are available for well-known protocols, as those listed below. Valid port range is **0** to **65535**.
range	Customizes timeout intervals for a range of TCP or UDP ports.
<beginning port>/<ending port>	Specifies the range of ports, to which to apply the timeout value; valid only for specifying TCP and UDP services. Valid ports range between **0** and **65535**.
	The following is the list of TCP port numbers that may be identified using the text name (in **bold**):

bgp (Port 179)	**kshell** (Port 544)
chargen (Port 19)	**login** (Port 513)
cmd (Port 514)	**lpd** (Port 515)
daytime (Port 13)	**nntp** (Port 119)
discard (Port 9)	**pim-auto-rp** (Port 496)
domain (Port 53)	**pop2** (Port 109)
echo (Port 7)	**pop3** (Port 110)
exec (Port 512)	**smtp** (Port 25)
finger (Port 79)	**ssh** (Port 22)
ftp (Port 21)	**sunrpc** (Port 111)
ftp-data (Port 20)	**tacacs** (Port 49)
gopher (Port 70)	**talk** (Port 517)
hostname (Port 101)	**telnet** (Port 23)
https (Port 443)	**time** (Port 37)
ident (Port 113)	**uucp** (Port 540)
irc (Port 194)	**whois** (Port 43)
klogin (Port 543)	**www** (Port 80)

The following is the list of UDP port numbers that may be identified using the text name (in **bold**):

biff (Port 512)	**pim-auto-rp** (Port 496)
bootpc (Port 68	**rip** (Port 520)
bootps (Port 67)	**ripng** (Port 521)
discard (Port 9)	**snmp** (Port 161)
dnsix (Port 195)	**snmptrap** (Port 162))
domain (Port 53)	**sunrpc** (Port 111)
echo (Port 7)	**syslog** (Port 514)
isakmp (Port 500)	**tacacs** (Port 49)
mobile-ip (Port 434)	**talk** (Port 517)
nameserver (Port 42)	**tftp** (Port 69)
netbios-dgm (Port 138)	**time** (Port 37)
netbios-ns (Port 137)	**who** (Port 513)
netbios-ss (Port 139)	**xdmcp** (Port 177)
ntp (Port 123)	

vrf <*name*> Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to perform the policy timeout. If no VRF is specified, the action is performed on the default unnamed VRF.

Default Values

By default, policy session timeouts are set to **600** seconds for established TCP policy sessions, and **60** seconds for all other protocols.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the **ripng** option for UDP ports.

Functional Notes

This **ipv6 policy-timeout** command is used to configure the session timeout value for established policy sessions. Use the commands *ipv6 firewall rst-timeout <timeout> on page 1542*, *ipv6 firewall rst-timeout <timeout> on page 1542*, and *ipv6 firewall tcp-unestab-timeout <timeout> on page 1544* to configure timeout values for TCP FINISH (FIN), TCP RESET (RST), and pre-established TCP policy sessions.

Established TCP policy sessions are firewall sessions in which a three-way handshake has been observed, but no RST has been received by either endpoint, nor has a FIN been received from both endpoints. Established policy sessions can also be a stateless TCP policy session prior to the receipt of an RST from either endpoint or a FIN from both endpoints, or a policy session for all non-TCP protocols. Established policy session timeouts are configured to customize timeout intervals for protocols (by specifying the protocol or a specific access control list (ACL)), specific services (by specifying the port used or a specific ACL), and specific ingress policy classes. Multiple commands can be used to specify different timeouts for different protocols, services, and ingress policy classes.

Usage Examples

The following examples configure multiple policy session timeouts based on different protocols (and the associated ACLs):

(config)**#ipv6 policy-timeout match A1 policy P1 1000**
(config)**#ipv6 policy-timeout match A2 policy P1 2000**
(config)**#ipv6 policy-timeout tcp ssh policy P1 3000**
(config)**#ipv6 policy-timeout tcp range 100 200 policy P1 4000**
(config)**#ipv6 policy-timeout tcp range 150 250 policy P1 5000**
(config)**#ipv6 policy-timeout tcp all-ports policy P1 6000**
(config)**#ipv6 policy-timeout match A3 7000**
(config)**#ipv6 policy-timeout tcp ssh 8000**

(config)**#ipv6 access-list extended A1**
(config-ex6-nacl)**#permit gre host 2001:DB8:1234:1::1 any**
(config-ex6-nacl)**#permit tcp any any eq www**

(config)**#ipv6 access-list extended A2**
(config-ex6-nacl)**#permit tcp host 2001:DB8:1234:1::1 any**

(config)**#ipv6 access-list extended A3**
(config-ex6-nacl)**#permit esp any any**

ipv6 prefix-list <*name*> seq <*number*>

Use the **ipv6 prefix-list seq** command to specify an Internet Protocol version 6 (IPv6) prefix to be matched when filtering IPv6 routes. Use the **no** form of this command to remove a prefix list. Variations of this command include:

ipv6 prefix-list <*name*> **seq** <*number*> **deny** <*ipv6 address/prefix-length*>
ipv6 prefix-list <*name*> **seq** <*number*> **deny** <*ipv6 address/prefix-length*> **ge** <*value*>
ipv6 prefix-list <*name*> **seq** <*number*> **deny** <*ipv6 address/prefix-length*> **le** <*value*>
ipv6 prefix-list <*name*> **seq** <*number*> **permit** <*ipv6 address/prefix-length*>
ipv6 prefix-list <*name*> **seq** <*number*> **permit** <*ipv6 address/prefix-length*> **ge** <*value*>
ipv6 prefix-list <*name*> **seq** <*number*> **permit** <*ipv6 address/prefix-length*> **le** <*value*>

Syntax Description

<*name*>	Specifies a particular prefix list. Prefix list names can be up to **80** characters in length.
<*number*>	Specifies the entry's unique sequence number that determines the processing order. Lower numbered entries are processed first. Range is **1** to **4294967294**.
permit <*ipv6 address/prefix-length*>	Permits access to entries matching the specified network IPv6 address and the corresponding network prefix length. IPv6 addresses and prefixes are expressed in colon hexadecimal format (for example, **2001:DB8:0:3F3B::/64**).
deny <*ipv6 address/prefix-length*>	Denies access to entries matching the specified network IPv6 address and the corresponding network prefix length. IPv6 addresses and prefixes are expressed in colon hexadecimal format (for example, **2001:DB8:0:3F3B::/64**).
le <*value*>	Specifies the upper end of the range and indicates that the length must be less than or equal to the specified value in order to match. Range is **0** to **32**.
ge <*value*>	Specifies the lower end of the range and indicates that the length must be greater than or equal to the specified value in order to match. Range is **0** to **32**.

Default Values

If no **ge** or **le** parameters are specified, an exact match is assumed. If only **ge** is specified, the AOS device assumes 32 as the upper limit. If only **le** is specified, the AOS device assumes the network address's length as the lower limit.

Command History

Release 10.1.0	Command was introduced.

Functional Notes

This command specifies a prefix to be matched when filtering routes. Prefix lists can be useful in configurations of Border Gateway Protocol (BGP) to define the routes that an AOS device can advertise to or receive from a BGP address family (AF) neighbor. Common uses for prefix lists include: preventing a network from becoming a transit for external traffic when multihoming, receiving only routes from remote virtual private network (VPN) sites, prohibiting the advertisement of a network, and load balancing outbound traffic. When using this command, if the network address is entered without specifying a range for prefix lengths, the router assumes that the route must be an exact match.

Optionally, this command may specify a range of prefix lengths. The following rule must be followed: len < ge-value ≤ le-value. A filter that exactly matches a prefix length can be created by entering the length for both the **ge** and **le** values. A prefix list with no entries allows all routes. A route that does not match any entries in a prefix list is dropped. As soon as a route is permitted or denied, there is no further processing of the rule in the prefix list. A route that is denied with the initial entry of a prefix list will not be allowed, even if it matches a permitting entry further down the list.

Usage Examples

The following example creates a prefix list entry in the IPv6 prefix list TEST that allows all routes to prefixes in the **2001:DB8:0:3F3B::/64** network:

(config)**#ipv6 prefix-list TEST seq 5 permit 2001:DB8:0:3F3B::/64 le 24**

ipv6 route

Use the **ipv6 route** command to add an Internet Protocol version 6 (IPv6) static route to the IPv6 route table. Use the **no** form of this command to remove a configured IPv6 static route. To specify a route using a named prefix, refer to *ipv6 route named-prefix on page 1561*. Variations of this command include:

ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc]**
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc] tag** *<value>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc] track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* **| system-control-evc | system-management-evc] tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <administrative distance>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <administrative distance>* **tag** *<value>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <administrative distance>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <administrative distance>* **tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface>* **tag** *<value>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface>* **tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>* **tag** *<value>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>* **tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0**
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0 tag** *<value>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0 track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0 tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>* **tag** *<value>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>* **track** *<name>*
ipv6 route [vrf *<name>***]** *<ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>* **tag** *<value>* **track** *<name>*

Syntax Description

<ipv6 prefix/prefix length>	Specifies the network defined by this static route entry. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**. The IPv6 prefix cannot be a link-local address.
<ipv6 address>	Optional. Specifies the next-hop IPv6 address defined by the static route. This is not a link-local IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an egress interface on the router which connects to the next-hop IPv6 device on the path toward the specified network. Interfaces are entered in the *<interface> <slot/port | interface id>* format. You must use the *<interface>* parameter in conjunction with the next-hop IPv6 address if you are specifying a link-local IPv6 address (**FE80::**) as the next hop.
null 0	Optional. Specifies that traffic is routed to the null interface. The router drops all packets destined for the null interface. Use the null interface to allow the router to advertise a route, but not forward traffic to the route.
<administrative distance>	Optional. Specifies an administrative distance associated with the static route, and is used to determine the best route when multiple routes to the same destination exist. The route with the lowest administrative distance is the preferred route. Administrative distance range is **1** to **255**.
tag *<value>*	Optional. Specifies a number to use as a tag for this route. Valid range is **1** to **65535**.
track *<name>*	Optional. Enables tracking on the indicated route. Once the named track enters a fail state, the route specified by the command is disabled and traffic will no longer be routed using that route. For more information on configuring tracks, refer to *track <name> on page 1886*.
mef-ethernet *<slot/port>*	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-mangement-evc	Optional. Specifies the system management EVC. This EVC is preconfigured on the unit.
vrf *<name>*	Optional. Specifies to create the static route on a specific virtual routing and forwarding (VRF).

Default Values

By default, no static routes are added to the IPv6 route table. If a static route is created, the administrative distance is **1** by default.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.

Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the **track** parameter and MEF Ethernet interface.

Functional Notes

Each static route is only added to the IPv6 route table when the IPv6 interface is configured and in an UP state. There are three types of static routes that can be used: directly attached, recursive, and fully specified.

A directly attached static route is a route in which the next hop for the route is entered as an interface. Packets destined for the specified network are assumed to be directly reachable on the specified interface. If you are using a directly attached static route, and the interface you are using uses Layer 2 addresses (for example, as an Ethernet interface does), then address resolution is performed when a packet is delivered to the network. For Point-to-Point Protocol (PPP) interfaces, the packet is simply forwarded through the interface in the same way that a packet is forwarded when an IPv6 on-link prefix is defined at the interface.

A recursive static route is a route in which the next hop for the route is entered as the IPv6 address of the next-hop router. When a recursive static route is used, AOS attempts to determine the interface used to reach the next-hop address. Recursive routes are added to the route table only when the router has determined which interface to use for egress traffic.

A fully specified static route is a route in which the next hop is entered as an IPv6 address and an interface for the next-hop router is specified. This type of static route restricts the use of the route to the specified interface. A fully specified static route MUST be used when the next hop is specified by its link-local address, which alone has no context of location.

Usage Examples

The following example creates a static route in the IPv6 routing table that has a local-link next-hop address, egresses from the **ethernet 0/1** interface, includes a tag of **3**, and has an administrative distance of **2**:

(config)**#ipv6 route 2001:DB8:3F::/48 fe80::202:b3ff:fe1e:8345 ethernet 0/1 tag 3 2**

ipv6 route named-prefix

Use the **ipv6 route named-prefix** command to add an Internet Protocol version 6 (IPv6) static route to the IPv6 route table using a named prefix. Use the **no** form of this command to remove a configured IPv6 static route. To specify a route without using a named prefix, refer to *ipv6 route on page 1558*. Variations of this command include:

ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* | **system-control-evc | system-management-evc]**
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* | **system-control-evc | system-management-evc] tag** *<value>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* | **system-control-evc | system-management-evc] track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **[mef-ethernet** *<slot/port>* | **system-control-evc | system-management-evc] tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <administrative distance>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <administrative distance>* **tag** *<value>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <administrative distance>* **track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <administrative distance>* **tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface>* **tag** *<value>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface>* **track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface>* **tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>* **tag** *<value>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>* **track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address> <interface> <administrative distance>* **tag** *<value>* **track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0**
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0 tag** *<value>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0 track** *<name>*
ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0**

tag *<value>* **track** *<name>*

ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>*

ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>* **tag** *<value>*

ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>* **track** *<name>*

ipv6 route [vrf *<name>***] named-prefix** *<prefix-name> <ipv6 prefix/prefix length> <ipv6 address>* **null 0** *<administrative distance>* **tag** *<value>* **track** *<name>*

Syntax Description

<prefix name>	Specifies a route is created using a named prefix. The *<prefix name>* parameter specifies the prefix variable name.
<ipv6 prefix/prefix length>	Specifies the network defined by this static route entry. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**. The IPv6 prefix cannot be a link-local address.
<ipv6 address>	Specifies the next-hop IPv6 address defined by the static route. This is not a link-local IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an egress interface on the router which connects to the next-hop IPv6 device on the path toward the specified network. Interfaces are entered in the *<interface> <slot/port* | *interface id>* format. You must use the *<interface>* parameter in conjunction with the next-hop IPv6 address if you are specifying a link-local IPv6 address (**FE80::**) as the next hop.
null 0	Optional. Specifies that traffic is routed to the null interface. The router drops all packets destined for the null interface. Use the null interface to allow the router to advertise a route, but not forward traffic to the route.
<administrative distance>	Optional. Specifies an administrative distance associated with the static route, and is used to determine the best route when multiple routes to the same destination exist. The route with the lowest administrative distance is the preferred route. Administrative distance range is **1** to **255**.
tag *<value>*	Optional. Specifies a number to use as a tag for this route. Valid range is **1** to **65535**.
track *<name>*	Optional. Enables tracking on the indicated route. Once the named track enters a fail state, the route specified by the command is disabled and traffic will no longer be routed using that route. For more information on configuring tracks, refer to *track <name> on page 1886*.
mef-ethernet *<slot/port>*	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC). This EVC is preconfigured on the unit.
system-management-evc	Optional. Specifies the system management EVC. This EVC is preconfigured on the unit.

vrf <*name*>	Optional. Specifies to create the static route on a specific virtual routing and forwarding (VRF).

Default Values

By default, no static routes are added to the IPv6 route table. If a static route is created, the administrative distance is **1** by default.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the **track** parameter and MEF Ethernet interface.

Functional Notes

Each static route is only added to the IPv6 route table when the IPv6 interface is configured and in an UP state. There are three types of static routes that can be used: directly attached, recursive, and fully specified.

A directly attached static route is a route in which the next hop for the route is entered as an interface. Packets destined for the specified network are assumed to be directly reachable on the specified interface. If you are using a directly attached static route, and the interface you are using uses Layer 2 addresses (for example, as an Ethernet interface does), then address resolution is performed when a packet is delivered to the network. For Point-to-Point Protocol (PPP) interfaces, the packet is simply forwarded through the interface in the same way that a packet is forwarded when an IPv6 on-link prefix is defined at the interface.

A recursive static route is a route in which the next hop for the route is entered as the IPv6 address of the next-hop router. When a recursive static route is used, AOS attempts to determine the interface used to reach the next-hop address. Recursive routes are added to the route table only when the router has determined which interface to use for egress traffic.

A fully specified static route is a route in which the next hop is entered as an IPv6 address and an interface for the next-hop router is specified. This type of static route restricts the use of the route to the specified interface. A fully specified static route MUST be used when the next hop is specified by its link-local address, which alone has no context of location.

Usage Examples

The following example creates a static route named **PREFIX1** in the IPv6 routing table that has a local-link next-hop address, egresses from the **ethernet 0/1** interface, includes a tag of **3**, and has an administrative distance of **2**:

(config)**#ipv6 route named-prefix PREFIX1 2001:DB8:3F::/48 fe80::202:b3ff:fe1e:8345 ethernet 0/1 tag 3 2**

ipv6 unicast-routing

Use the **ipv6 unicast-routing** command to enable Internet Protocol version 6 (IPv6) unicast routing and specify the router as an IPv6 neighbor. Use the **no** form of this command to disable the IPv6 routing subsystem, remove any routing protocol entries from the IPv6 routing table, cease IPv6 routing functions, and disable IPv6 unicast routing.

Syntax Description

No subcommands.

Default Values

By default, IPv6 unicast routing is disabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

This **ipv6 unicast-routing** command functions similarly to the **ip routing** command for IPv4 services. In order to enable IPv6 unicast routing, you must first configure interfaces to use IPv6 before IPv6 communication takes place. When IPv6 unicast routing is enabled globally, the router flag is set to **1** in neighbor advertisement (NA) messages.

Using the **no** form of this command disables the IPv6 routing subsystem, removes any routing protocol entries from the IPv6 route table, causes IPv6 routing functions to cease, and disables IPv6 unicast routing. In addition, NA

messages are sent at each interface indicating the neighbor is no longer a router (router flag is set to **0**), and that the router is no longer the default router for any advertised prefixes. When IPv6 unicast routing is disabled, the existing IPv6 configuration is retained, but no IPv6 packets are routed and no routing resources are consumed.

If IPv6 unicast routing is not enabled, but an interface has IPv6 enabled, that interface may communicate as an IPv6 host to other devices. If IPv6 packets are received that are not addressed to that interface, the packets are dropped.

Usage Examples

The following example enables IPv6 unicast routing and specifies the router as an IPv6 neighbor:

(config)**#ipv6 unicast-routing**

isdn-group <*number*>

Use the **isdn-group** command to enter the ISDN Group Configuration mode command set. Use the **no** form of this command to disable this feature. Refer to the section *Voice ISDN Group Command Set on page 4656* for more information on the commands available for each group.

Syntax Description

<number>	Specifies the integrated services digital network (ISDN) group. Range is **1** to **255**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Functional Notes

An ISDN group allows the user to specify the maximum and minimum number of B-channels that can be used for a specific type of call. It is a logical group of B-channels from one or more ISDN interfaces. The interfaces can be of different types (e.g., primary rate interface (PRI) and basic rate interface (BRI)). An ISDN interface can be a member of multiple ISDN groups that makes it possible to share its B-channels between different types of calls.

Usage Examples

The following example uses the **isdn-group** command to enter the ISDN Group Configuration mode for ISDN group 1:

```
(config)#isdn-group 1
(config-isdn-group 1)#
```


isdn-number-template

Use the **isdn-number-template** command to create an entry in the integrated services digital network (ISDN) number-type template that is used when encoding the called party and calling party information elements (IEs) for inbound and outbound ISDN calls. Use the **no** form of this command to delete the configured entry. Variations of this command include the following:

isdn-number-template <*template id*> **prefix** <*number*> **abbreviated** <*pattern*>
isdn-number-template <*template id*> **prefix** <*number*> **international** <*pattern*>
isdn-number-template <*template id*> **prefix** <*number*> **national** <*pattern*>
isdn-number-template <*template id*> **prefix** <*number*> **network-specific** <*pattern*>
isdn-number-template <*template id*> **prefix** <*number*> **plan** <*indicator*> **type** <*number*> <*pattern*>
isdn-number-template <*template id*> **prefix** <*number*> **subscriber** <*pattern*>
isdn-number-template <*template id*> **prefix** <*number*> **unknown** <*pattern*>

Syntax Description

<*template id*>	Specifies a numeric identifier for the template entry. Valid range is **1** to **255**.
prefix <*number*>	Specifies the expected prefix for the call type. Prefixes can be left blank (using double quotation marks " "), or consist of unlimited length strings of zeros and ones. For example, for international calls made from within the United States, a prefix of 011 is expected.
abbreviated	Specifies using **abbreviated** (bits 110) in the type of number (TON) octet. Abbreviated is used mainly in private ISDN network applications and the implementation is network dependent.
international	Specifies using **international** (bits 001) in the TON octet. International is used for calls destined outside the national calling area. International calls have the international direct dialing (IDD) prefix removed. For example, consider an international call of 011-N$, where the IDD prefix is 011 and the N$ represents the digits necessary for routing the call at the destination. When the called party IE is created for this call, the prefix is stripped and the N$ digits are placed in the number digits field.
national	Specifies using **national** (bits 010) in the TON octet. National is used for calls destined for inside the national calling area (i.e., does not cross into an international local access and transport area (LATA)). National calls have the direct dialing prefix removed. For example, consider a national call with a direct dialing prefix of 1 and NXX-NXX-XXXX to represent the ten-digit number necessary for routing the call. When the called party IE is created for this call, the prefix (1) is stripped and the NXX-NXX-XXXX digits are placed in the number digits field.

network-specific	Specifies using **network-specific** (bits 011) in the TON octet. Network-Specific is used for calls that require special access to a private network, which requires the use of a prefix that should be stripped once access to the network has been gained. Network-specific calls have the dialing prefix removed. For example, a call to a private network with the 700 consists of 700-N$, where 700 is the dialing prefix and N$ represents the digits necessary for routing the call at the destination. When the Called Party IE is created for this call, the prefix is stripped and the N$ is placed in the Number Digits field.
plan <*indicator*>	Specifies the numbering plan indicator (NPI) to use in combination with the TON and associate it with a number pattern. Valid range is **0** to **15**.
subscriber	Specifies using **subscriber** (bits 100) in the TON octet. Subscriber is used for local calls (not long distance). Subscriber calls, by default, have the area code removed. For example, a subscriber call to 916-555-1212 would have the prefix 916 stripped and 555-1212 in the number digits field. For areas with mandatory ten-digit dialing, a blank prefix should be entered to ensure that all ten digits are passed to the number digits field.
type <*number*>	Specifies the TON to use in combination with the NPI and associate it with a number pattern. Valid range is **0** to **7**.
unknown	Specifies using **unknown** (bits 000) in the TON octet. Unknown is used when the number type is not known. Unknown numbers are assumed to have no prefix, and the entire dialed number is presented in the number digits field.
<*pattern*>	Specifies a pattern for this template. Refer to *Functional Notes* for more information.

Default Values

By default, the following number template for domestic emergency calls (911) is the only template preconfigured in AOS:

isdn-number-template 0 prefix “ ” subscriber 911

Command History

Release 11.1	Command was introduced.
Release A4.05	Command was expanded to include the **plan** <*indicator*> **type** <*number*> <*pattern*> parameter.

Functional Notes

The command **isdn-number-template** <*template id*> **prefix** <*number*> **plan** <*indicator*> **type** <*number*> <*pattern*> is used to associate any combination of NPIs and TONs with a number pattern. Not all combination values are allowed, and AOS does not check the entry validity. Refer to the International Telecommunication Union (ITU) recommendation Q.931 for the most current information.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example creates a number template (labeled **1**) and prefix (labeled **1**) for national calls:

(config)**#isdn-number-template 1 prefix 1 national Nxx-Nxx-xxxx**

led status-led startup-state

Use the **led status-led startup-state** command to control the state of the status LED upon system startup of an applicable AOS device. This command can be used to turn off the LED, as well as control both the LED color and blink rate. Use the **no** form of this command to return to the default setting. Variations of this command include:

led status-led startup-state [green | red]
led status-led startup-state [green | red] blink [fast | slow]
led status-led startup-state red-green
led status-led startup-state off

Syntax Description

green	Modifies the status LED display to green.
red	Modifies the status LED display to red.
red-green	Modifies the status LED to alternate between red and green
blink	Specifies the status LED blink rate. If the blink rate is not specified, the display color will be solid (i.e., non-blinking).
fast	Specifies a blink rate of five times per second.
slow	Specifies a blink rate of once per second.
off	Turns off the status LED.

Default Values

By default, the status LED is solid green.

Command History

Release R11.7.0	Command was introduced.

Functional Notes

This command only controls the state of the LED upon startup; it does not alter the current state of the status LED.

Usage Examples

The following example changes the startup state of the status LED display to slow, blinking red:

(config)**#led status-led startup-state red blink slow**

license server

Use the **license server** command to configure a license server, from which license keys are automatically retrieved by the AOS unit. This command must be issued before using the command *license activate <activation key> on page 500* to activate AOS feature licenses. Use the **no** form of this command to remove the license server configuration and return to the default server. Variations of this command include:

license server url *<url>*
license server vrf *<name>* **url** *<url>*

Syntax Description

url *<url>*	Specifies the uniform resource locator (URL) address of the license server. Specify the URL using either Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS), for example, **https://example.com**.
vrf *<name>*	Optional. Specifies a non-default virtual routing and forwarding (VRF) instance on which to configure the license server.

Default Values

If no license server is configured, a license key request is automatically sent to **https://portal.adtran.com/web/ptapi/generate**.

Command History

Release R13.4.0	Command was introduced.

Functional Notes

The server configured with the command is used in conjunction with the command *license activate <activation key> on page 500*. The activation keys used with the **license activate** command are provided to you when you purchase licenses for additional AOS features. When the **license activate** command is issued, the entered activation keys are automatically sent to the licensing server configured with the **license server** command, and then the features are automatically licensed on the AOS unit.

This two-step licensing procedure replaces the four-step licensing process introduced in AOS firmware release R11.8.0. For more information about the AOS feature licensing process, refer to the quick start guide, *Licensing AOS Features*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures a license server with the URL **https://example.com**, on the default VRF, for use with AOS feature license activation keys:

(config)**#license server url https://example.com**

line

Use the **line** command to enter the line configuration for the specified console, Telnet, or secure shell (SSH) session. Refer to the sections *Line (Console) Interface Command Set on page 2021*, *Line (Telnet) Interface Command Set on page 2054*, and *Line (SSH) Interface Command Set on page 2038* for information on the subcommands. Variations of this command include:

line console *<line number>*
line ssh *<line number>*
line ssh *<line number> <ending number>*
line telnet *<line number>*
line telnet *<line number> <ending number>*

Syntax Description

console	Enters the configuration mode for the DB-9 (female) **CONSOLE** port located on the rear panel of the unit. Refer to the section *Line (Console) Interface Command Set on page 2021* for information on the subcommands found in that command set.
telnet	Enters the configuration mode for Telnet session(s), allowing you to configure for remote access. Refer to the section *Line (Telnet) Interface Command Set on page 2054* for information on the subcommands found in that command set.
ssh	Enters the configuration mode for SSH. Refer to the section *Line (SSH) Interface Command Set on page 2038* for information on the subcommands found in that command set.
<line number>	Specifies the starting session to configure for remote access. Valid range for console is **0**. Valid range for Telnet and SSH is **0** to **4**. If configuring a single Telnet or SSH session, enter a single line number.
<ending number>	Optional. Specifies the last Telnet or SSH session to configure for remote access. Valid range is **0** to **4**. For example, to configure all available Telnet sessions, enter **line telnet 0 4**.

Default Values

By default, there are no configured Telnet or SSH sessions. By default, the AOS line console parameters are configured as follows:

Data Rate: 9600
Data bits: 8
Stop bits: 1
Parity Bits: 0
No flow control

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the SSH.

Usage Examples

The following example begins the configuration for the **CONSOLE** port located on the rear of the unit:

```
(config)#line console 0
(config-con0)#
```

The following example begins the configuration for all available Telnet sessions:

```
(config)#line telnet 0 4
(config-telnet0-4)#
```

The following example begins the configuration for all available SSH sessions:

```
(config)#line ssh 0 4
(config-ssh0-4)#
```

lldp

Use the **lldp** command to configure global settings that control the way Link Layer Discovery Protocol (LLDP) functions. Use the **no** form of this command to return to the default setting. Variations of this command include:

lldp med-fast-start-interval <*value*>
lldp minimum-transmit-interval <*value*>
lldp reinitialization-delay <*value*>
lldp system-capabilities exclude telephone
lldp transmit-interval <*value*>
lldp ttl-multiplier <*value*>

Syntax Description

med-fast-start-interval	Specifies the fast start transmit interval (in seconds) that LLDP-Media Endpoint Discovery (LLDP-MED) time length values (TLVs) are sent once every second, allowing rapid automatic configuration of LLDP-MED capable endpoints at startup. Range is **1** to **10** seconds. Default value is 4 seconds.
minimum-transmit-interval	Defines the minimum amount of time between transmission of LLDP frames in seconds. Range is **1** to **8192** seconds.
reinitialization-delay	Defines the minimum amount of time to delay after LLDP is enabled on a port before allowing transmission of additional LLDP frames on that port in seconds. Range is **1** to **10** seconds.
system-capabilities	Configures local system capabilities.
exclude telephone	Excludes telephone flag in the system capabilities TLV. Enabling this command prevents the AOS unit from advertising the telephone system capabilities in both the system capabilities and enabled capabilities portions of the LLDP packet.
transmit-interval	Defines the delay between LLDP frame transmission attempts during normal operation in seconds. Range is **5** to **32768** seconds.
ttl-multiplier	Defines the time to live (TTL) multiplier to be applied to the transmit interval to compute the time to live for data sent in an LLDP frame. Range is **2** to **10**.
<*value*>	Specifies the interval, delay, or multiplier.

Default Values

By default, **med-fast-start-interval** is **4** seconds; **minimum-transmit-interval** is **2** seconds; **reinitialization-delay** is **2** seconds; **transmit-interval** is **30** seconds; and **ttl-multiplier** is **4**.

Command History

Release 8.1	Command was introduced.
Release 17.2	Command was expanded to include the **med-fast-start-interval** parameter.
Release A5.01	Command was expanded to include the **system-capabilities** and **exclude telephone** parameters.

Functional Notes

Once a device receives data from a neighboring device in an LLDP frame, it will retain that data for a limited amount of time. This amount of time is called time to live, and it is part of the data in the LLDP frame. The time to live transmitted in the LLDP frame is equal to the transmit interval multiplied by the TTL multiplier.

Usage Examples

The following example sets the LLDP minimum transmit interval to **10** seconds:

(config)**#lldp minimum-transmit-interval 10**

The following example sets the LLDP reinitialization delay to **5** seconds:

(config)**#lldp reinitialization-delay 5**

The following example sets the LLDP transmit interval to **15** seconds:

(config)**#lldp transmit-interval 15**

The following example sets the LLDP transmit interval to **15** seconds and the TTL multiplier to **2** for all LLDP frames transmitted from the unit. The resulting TTL is 30 seconds:

(config)**#lldp transmit-interval 15**
(config)**#lldp ttl-multiplier 2**

load-protect

Use the **load-protect** command to enable and configure load-protect CPU throttling. Variations of this command include:

load-protect background rate-limit
load-protect background rate-limit <*increase percentage*> <*decrease percentage*>
load-protect background interval <*value*> **rate-limit**
load-protect background interval <*value*> **rate-limit** <*increase percentage*> <*decrease percentage*>
load-protect cli rate-limit
load-protect cli rate-limit <*increase percentage*> <*decrease percentage*>
load-protect cli interval <*value*> **rate-limit**
load-protect cli interval <*value*> **rate-limit** <*increase percentage*> <*decrease percentage*>

Syntax Description

background	Specifies the scope of the command is all encompassing.
cli	Specifies the scope of the command is limited to the command line interface.
interval <*value*>	Optional. Sets the maximum latency, in milliseconds, allowed to occur before declaring the CLI or background in congestion.
rate-limit	Specifies that load protect be enabled utilizing a simple step function, unless a percentage of increase and decrease are defined.
<*increase percentage*>	Optional. Sets the percentage increase to be added to the current percentage of packets that the CPU handles.
<*decrease percentage*>	Optional. Sets the percentage decrease to be removed from the current percentage of packets that the CPU handles.

Default Values

If no **interval** <*value*> is entered, the command defaults to a simple step function to throttle high CPU utilization.

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example enables load protect for the CLI with a maximum latency of 200 ms:

(config)**#load-protect cli interval 200 rate limit**

load-protect protocol

Use the **load-protect protocol** command to enable and configure a specified protocol's queue and values for the load protect feature's protocol rate limiter. Variations of this command include:

load-protect protocol arp cbs <*number*>
load-protect protocol arp cir <*number*>
load-protect protocol arp queue <*number*>
load-protect protocol default cir <*number*>
load-protect protocol default cir <*number*> **cbs** <*number*>
load-protect protocol dhcp cbs <*number*>
load-protect protocol dhcp cir <*number*>
load-protect protocol dhcp queue <*number*>
load-protect protocol icmp cbs <*number*>
load-protect protocol icmp cir <*number*>
load-protect protocol icmp queue <*number*>
load-protect protocol icmp-unreachable cbs <*number*>
load-protect protocol icmp-unreachable cir <*number*>
load-protect protocol icmp-unreachable queue <*number*>
load-protect protocol ipv6-hop-by-hop cbs <*number*>
load-protect protocol ipv6-hop-by-hop cir <*number*>
load-protect protocol ipv6-hop-by-hop queue <*number*>
load-protect protocol ipv6-nd cbs <*number*>
load-protect protocol ipv6-nd cir <*number*>
load-protect protocol ipv6-nd queue <*number*>
load-protect protocol ntp cbs <*number*>
load-protect protocol ntp cir <*number*>
load-protect protocol ntp queue <*number*>
load-protect protocol radius cbs <*number*>
load-protect protocol radius cir <*number*>
load-protect protocol radius queue <*number*>
load-protect protocol snmp cbs <*number*>
load-protect protocol snmp cir <*number*>
load-protect protocol snmp queue <*number*>
load-protect protocol ssh cbs <*number*>
load-protect protocol ssh cir <*number*>
load-protect protocol ssh queue <*number*>
load-protect protocol vrrp cbs <*number*>
load-protect protocol vrrp cir <*number*>
load-protect protocol vrrp queue <*number*>
load-protect protocol vrrpv3 cbs <*number*>
load-protect protocol vrrpv3 cir <*number*>
load-protect protocol vrrpv3 queue <*number*>

Syntax Description

arp	Specifies internet protocol version 4 (IPv4) Address Resolution Protocol (ARP) packets.
default	Specifies the feature behavior for packets not specified by another protocol.
dhcp	Specifies Dynamic Host Configuration Protocol version 4 (DHCPv4) and DHCPv6 packets.
icmp	Specifies all IPv4 and IPv6 Internet Control Message Protocol (ICMP) packets, except for unreachables.
icmp-unreachable	Specifies IPv4 and IPv6 ICMP unreachable packets.
ipv6-hop-by-hop	Specifies any IPv6 packet with a hop-by-hop option correctly set on the packet.
ipv6-nd	Specifies IPv6 neighbor discovery packets.
ntp	Specifies Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) packets.
radius	Specifies Remote Authentication Dial-in User Service (RADIUS) packets.
snmp	Specifies Simple Network Management Protocol (SNMP) packets.
ssh	Specifies Secure Shell (SSH), Session Control Protocol (SCP) packets.
vrrp	Specifies Virtual Router Redundancy Protocol version 2 (VRRPv2) packets.
vrrpv3	Specifies VRRPv3 packets.
cbs <*number*>	Specifies the committed burst size (CBS) for the given protocol in number of packets.
cir <*number*>	Specifies the packet per second committed information rate (CIR) that is rate limited to the CPU for the given protocol.
queue <*number*>	Specifies the destination queue for the given protocol.

Default Values

By default the load protect feature is not enabled.

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example enables queue number **1** for all DHCPv4 and DHCPv6 packets whose CBS and CIR values may then be configured:

(config)**#load-protect protocol dhcp queue 1**

load-protect queue <*number*> weight packet <*weight*>

Use the **load-protect queue weight packet** command to set the weighted round robin (WRR) weight in packets per second for the specified queue.

Syntax Description

<*number*>	Specifies the desired queue.
<*weight*>	Specifies the WRR weight in packets per second.

Default Values

No default values are necessary for this command.

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example sets the number of packets per second to **50** for queue number **1**:

(config)**#load-protect queue 1 weight packet 50**

local *<start ip address> <end ip address>* **global** *<start ip address> <end ip address>*

Use the **local global** command to define local and global network range of addresses for static 1:1 network address translation (NAT) mapping. This command is entered from within the NAT pool's configuration command set by using the **ip nat pool** command. Refer to *ip nat pool <name> on page 1433* for more information.

Syntax Description

<start ip address>	Specifies the first IP address in the range.
<end ip address>	Specifies the last IP address in the range. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

No default values are necessary for this command.

Command History

Release 17.4	Command was introduced.

Functional Notes

Static pools define a local network range of addresses whose size must be equal to the global range. Source NAT will translate from the local range to the global range. Destination NAT will translate from the global range to the local range. The addresses do not have to start at the same offset. If this command is entered and the two ranges are not of the same size, an error message is displayed. The command will fail and the pool will remain in its original state. If the pool was configured with an existing address range prior to issuing the failed command, that range will remain unchanged. If no address range was present, the pool will remain incomplete.

In some situations, an address needs to be excluded that falls within a range. For example, suppose you are excluding 10.1.1.10 because it is the address used for many-to-one source NAT for other nonstatic NAT hosts. This can be accomplished by creating multiple pools. This configuration requires multiple policy class entries, but each can use the same access control list (ACL).

Usage Examples

The following example creates a static NAT pool named **POOL1** and defines the local range from **10.1.1.1** to **10.1.1.12** and the global range as **192.168.1.1** to **192.168.1.12**:

(config)**#ip nat pool POOL1 static**
(config-natpool)**#local 10.1.1.1 10.1.1.12 global 192.168.1.1 192.168.1.12**

The following example creates two static NAT pools named **POOL1** and **POOL2**. This example defines the local range from **10.1.1.1** to **10.1.1.254** and the global range as **192.168.1.1** to **192.168.1.254** while excluding the address **10.1.1.10**:

(config)**#ip nat pool POOL1 static**
(config-natpool)**#local 10.1.1.1 10.1.1.9 global 192.168.1.1 192.168.1.9**
(config)**#ip nat pool POOL2 static**
(config-natpool)**#local 10.1.1.11 10.1.1.254 global 192.168.1.11 192.168.1.254**

logging console

Use the **logging console** command to enable AOS to log events to all consoles. Use the **no** form of this command to disable console event logging.

Syntax Description

No subcommands.

Default Values

By default, logging console is disabled.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables AOS to log events to all consoles:

(config)**#logging console**

logging email address-list <*email address*> ; <*email address*>

Use the **logging email address-list** command to specify one or more email addresses that will receive event notification. The criteria for event matching is configured using the command *logging email priority-level on page 1589*. Use the **no** form of this command to remove a listed address.

Syntax Description

<email address>	Specifies the complete email address to use when sending logged messages. (This field allows up to 256 characters.) Enter as many email addresses as desired, placing a semi-colon (;) between addresses.

Default Values

By default, there are no configured logging email addresses.

Command History

Release 1.1	Command was introduced.

Functional Notes

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example specifies three email addresses to use when sending logged messages:

(config)#**logging email address-list**
admin@adtranemail.com;ntwk@adtranemail.com;support@adtranemail.com

logging email error-report address-list *<email address>* ; *<email address>*

Use the **logging email error-report address-list** command to specify one or more email addresses to receive exception reports and Hypertext Transfer Protocol (HTTP) error reports for use in troubleshooting. Use the **no** form of this command to remove a listed address.

Syntax Description

<email address>	Specifies the email address(es) to use when sending exception and HTTP error reports. This field allows up to 256 characters. Enter as many email addresses as desired, placing a semi-colon (;) between each address.

Default Values

By default, there are no configured logging email addresses.

Command History

Release R11.1	Command was introduced
Release R10.8.0	Command changed from **logging email exception-report address-list** to **logging email error-report address-list**.

Functional Notes

When AOS experiences an exception, it will generate a file with detailed information that Adtran's Technical Support can use to diagnose the problem. This command allows the unit to email the exception report to a list of addresses upon rebooting after the exception. In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example will enable exception report forwarding to **john.doe@company.com** using the **1.1.1.1** SMTP email server:

(config)#**logging email error-report address-list john.doe@company.com**

logging email ip urlfilter top-websites

Use the **logging email ip urlfilter top-websites** command to specify the parameters for receiving top websites reports via email. Use the **no** form of this command to disable top websites reporting email notification. Variations of this command include:

logging email ip urlfilter top-websites address-list *<email addresses>*
logging email ip urlfilter top-websites send-time *<HH:MM:SS>*

Syntax Description

address-list	Specifies the configuration of a list of email addresses to receive top websites reports.
send-time	Specifies the configuration of when email reports for top websites will be sent.
<email addresses>	Specifies the complete email address to use when sending top websites reports. (This field allows up to 256 characters.) Enter as many email addresses as desired, placing a semi-colon (;) between addresses.
<HH:MM:SS>	Specifies the hours, minutes, and seconds in a 24-hour format for sending top websites reports by email.

Default Values

By default, there are no configured logging email addresses or times for top websites reporting.

Once an address list is specified and top websites email reports are enabled, the default send-time for the reports is 12:00 a.m.

Command History

Release 16.1	Command was introduced.

Functional Notes

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.

- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example configures top websites reports to be emailed to **sys.admin@adtran.com** at 5:30 a.m.:

(config)**#logging email ip urlfilter top-websites address-list sys.admin@adtran.com**
(config)**#logging email ip urlfilter top-websites send-time 05:30:00**

logging email max-queue-depth

Use the **logging email max-queue-depth** to specify the maximum number of queued email messages awaiting delivery via Simple Mail Transfer Protocol (SMTP). Messages generated when the queue is full will be discarded without notification (except for the exception report email, which is always permitted in the queue). Variations of this command include:

logging email max-queue-depth
logging email max-queue-depth <*value*>

Syntax Description

<value>	Optional. Specifies the maximum number of email messages allowed in the queue.

Default Values

By default, 100 messages are allowed in the queue.

Command History

Release A5.01	Command was introduced.

Functional Notes

If messages are being generated faster than the SMTP client (or connected server) can process the messages, the queue will become filled and subsequent messages will be discarded without notification. In this case, the events causing the large number of messages to be generated should be investigated and addressed, the severity threshold for email logging should be adjusted using the command *logging email priority-level on page 1589*, or the queue size should be adjusted using this command, depending on available memory resources.

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example specifies that 200 email messages are allowed in the queue:

(config)**#logging email max-queue-depth 200**

logging email on

Use the **logging email on** command to enable the AOS email event notification feature. Use the command *logging email address-list <email address> ; <email address> on page 1582* to specify email address(es) that will receive notification when an event is received. Refer to *logging email priority-level on page 1589* for defining matching the criteria. Use the **no** form of this command to disable the email notification feature.

Syntax Description

No subcommands.

Default Values

By default, email event notification is disabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

The domain name is appended to the sender name when sending event notifications. Refer to the command *domain-name <domain name> on page 1263* for related information.

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example enables the AOS email event notification feature:

(config)**#logging email on**

logging email priority-level

Use the **logging email priority-level** command to set the threshold for events sent to the addresses specified using the command *logging email address-list <email address> ; <email address> on page 1582*. All events with the specified priority or higher will be sent to all addresses in the list. The command *logging email on on page 1588* must be enabled. Use the **no** form of this command to return to the default priority. Variations of this command include:

logging email priority-level error
logging email priority-level fatal
logging email priority-level info
logging email priority-level notice
logging email priority-level warning

Syntax Description

Sets the minimum priority threshold for sending messages to email addresses specified using the **logging email address-list** command. The following priorities are available (ranking from lowest to highest):

error	Logs events with **error** and **fatal** priorities.
fatal	Logs only events with a **fatal** priority.
info	Logs all events.
notice	Logs events with **notice**, **warning**, **error**, and **fatal** priorities.
warning	Logs events with **warning**, **error**, and **fatal** priorities.

Default Values

By default, the **logging email priority-level** is set to **warning**.

Command History

Release 1.1	Command was introduced.

Functional Notes

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.

- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example sends all messages with **warning** level or greater to the email addresses listed using the **logging email address-list** command:

(config)**#logging email priority-level warning**

logging email receiver-ip *<ipv4 address | hostname>*

Use the **logging email receiver-ip** command to specify the IP address or host name of the email server to use when sending email event notification. Use the **no** form of this command to remove a configured address. Variations of this command include:

logging email receiver-ip *<ipv4 address | hostname>*
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.0**
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.0 allow-tls1.1**
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.0 allow-tls1.1 allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.0 allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.1**
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.1 allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0 allow-tls1.1**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0 allow-tls1.1 allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0 allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.1**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.1 allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-sslv3**
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0 allow-tls1.1 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0 allow-tls1.1 allow-sslv3 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.0 allow-sslv3 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.1 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-tls1.1 allow-sslv3 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **port** *<number>* **allow-sslv3 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.0 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.0 allow-tls1.1 auth-username** *<username>* **auth-password** *<password>*
logging email receiver-ip *<ipv4 address | hostname>* **allow-tls1.0 allow-tls1.1 allow-sslv3 auth-username** *<username>* **auth-password** *<password>*

logging email receiver-ip <*ipv4 address* | *hostname*> **allow-tls1.0 allow-sslv3 auth-username** <*username*> **auth-password** <*password*>
logging email receiver-ip <*ipv4 address* | *hostname*> **allow-tls1.1 auth-username** <*username*> **auth-password** <*password*>
logging email receiver-ip <*ipv4 address* | *hostname*> **allow-tls1.1 allow-sslv3 auth-username** <*username*> **auth-password** <*password*>
logging email receiver-ip <*ipv4 address* | *hostname*> **allow-sslv3 auth-username** <*username*> **auth-password** <*password*>

Syntax Description

<*ipv4 address* **|** *hostname*>	Specifies the IPv4 address or host name of the email server to use when sending logged messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
allow-tls1.0	Optional. Allows the email server to use Transport Layer Security protocol version 1.0. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the email server to use TLS protocol version 1.1. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the server to use SSLv3. If SSLv3 is enabled, TLS version 1.0 is automatically enabled.
auth-username <*username*>	Optional. Specifies the user name to use if your email server requires authentication.
auth-password <*password*>	Optional. Specifies the password to use if your email server requires authentication.
port <*number*>	Optional. Specifies the port number of the remote email server. Range is **1** to **65535**.

Default Values

By default, there are no configured email server addresses.

Command History

Release 1.1	Command was introduced.
Release 15.1	Command was expanded to include the **auth-username** and **auth-password** options.
Release 16.1	Command was expanded to include the port number specification option.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Functional Notes

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example specifies an email server (with IP address **172.5.67.99**) to use when sending logged messages:

(config)**#logging email receiver-ip 172.5.67.99**

logging email sender

Use the **logging email sender** command to specify the sender in an outgoing logging email message. This name will appear in the **From** field of the receiver's inbox. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Functional Notes

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example sets a sender for outgoing messages:

(config)#**logging email sender myUnit@myNetwork.com**

logging email smdr address-list *<email address>* ; *<email address>*

Use the **logging email smdr address-list** command to specify one or more email addresses that will receive notification when the station messaging detail record (SMDR) log had reached 80 percent of its total capacity. Use the **no** form of this command to remove a listed address.

Syntax Description

<email address>	Specifies the complete email address to use when sending logged SMDR messages. (This field allows up to 256 characters.) Enter as many email addresses as desired, placing a semi-colon (;) between addresses.

Default Values

By default, there are no configured logging email addresses.

Command History

Release A5.01	Command was introduced.

Functional Notes

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.
- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface> on page 1596*.

Usage Examples

The following example specifies three email addresses to use when sending logged SMDR messages:

(config)#**logging email smdr address-list**
admin@adtranemail.com;ntwk@adtranemail.com;support@adtranemail.com

logging email source-interface *<interface>*

Use the **logging email source-interface** command to use the specified interface as the source for email messages transmitted by the unit. Use the **no** form of this command if you do not wish to override the normal source IP address.

Syntax Description

<interface>	Specifies the interface to be used as the source for email messages. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **logging email source-interface ?** for a complete list of valid interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

In order for the unit to send logging emails, the following features must be configured on the unit using the associated commands:

- The primary and secondary Domain Name System (DNS) server IP address must be configured using the command *name-server on page 1622*.
- Domain name lookup for DNS entries must be enabled using the command *domain-lookup on page 1261*.
- Event history logging must be enabled using the command *event-history on on page 1299*.
- Email logging must be enabled using the command *logging email on on page 1588*.
- The IPv4 address or host name of the SMTP mail server used for sending logging emails must be configured using the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.

- The sender (From address) of the logging email must be configured using the command *logging email sender on page 1594*.
- The source interface for communicating with the SMTP server must be specified using the command *logging email source-interface <interface>*.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for email messages:

(config)**#logging email source-interface loopback 1**

logging facility *<type>*

Use the **logging facility** command to specify a syslog facility type for the syslog server. Error messages meeting specified criteria are sent to the syslog server. For this service to be active, the command *logging forwarding on on page 1600* must be enabled. Use the **no** form of this command to return to the default setting.

Syntax Description

<type>	Specifies the syslog facility type. The following is a list of valid facility types:	
	auth	Authorization system
	cron	Cron facility
	daemon	System daemon
	kern	Kernel
	local0 - local7	Reserved for locally defined messages
	lpr	Line printer system
	mail	Mail system
	news	USENET news
	sys9 - sys14	System use
	syslog	System log
	user	User process
	uucp	UNIX-to-UNIX copy system

Default Values

The default value is **local7**.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example configures the syslog facility to the cron facility type:

(config)**#logging facility cron**

logging forwarding auxiliary-receiver-ip *<ipv4 address>*

Use the **logging forwarding auxiliary-receiver-ip** command to specify the IPv4 address of a secondary syslog server to use when logging events that match the criteria configured using the command *logging forwarding priority-level on page 1602*. This command can be applied to the default virtual private network (VPN) routing and forwarding (VRF) instance or a specific VRF instance. Use the **no** form of this command to remove an auxiliary receiver server address. Variations of this command include:

logging forwarding auxiliary-receiver-ip *<ip address>*
logging forwarding vrf *<name>* **auxiliary-receiver-ip** *<ip address>*

Syntax Description

<ipv4 address>	Specifies the IPv4 address of a secondary syslog server to use when logging messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrf *<name>*	Optional. Specifies a nondefault VRF instance on which the secondary syslog server is located. If no VRF instance is specified, the default unnamed VRF instance is assumed.

Default Values

By default, no secondary syslog servers are configured.

Command History

Release 17.7	Command was introduced.
Release A4.05	Command was introduced in AOS voice products.
Release R11.4.0	Command was expanded to include the **vrf** parameter.

Functional Notes

Configuring a secondary syslog server allows the redundant transmission of messages to two different servers. This server configuration is optional, and does not function as a failover address; therefore, the primary server should always be configured using the command *logging forwarding receiver-ip <ipv4 address> on page 1603*. Syslog transmits to this auxiliary address independently of normal server addresses.

Usage Examples

The following example specifies that messages are logged to both a primary syslog server (**172.5.67.99**) and an auxiliary syslog server (**172.5.69.100**):

(config)**#logging forwarding receiver-ip 172.5.67.99**
(config)**#logging forwarding auxiliary-receiver-ip 172.5.69.100**

logging forwarding on

Use the **logging forwarding on** command to enable the AOS syslog event feature. Use the command *logging forwarding priority-level on page 1602* to specify the event matching criteria used by AOS to determine whether a message should be forwarded to the syslog server. Use the **no** form of this command to disable the syslog event feature.

Syntax Description

No subcommands.

Default Values

By default, syslog event notification is disabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the AOS syslog event feature:

(config)**#logging forwarding on**

logging forwarding debug <*line*>

Use the **logging forwarding debug** command to send debug messages for various protocols and features to the AOS syslog server. Use the **no** form of this command to disable debug messages in the syslog server.

Turning on a large amount of debug information can adversely affect the performance of your unit.

Syntax Description

<line>	Specifies the protocol or feature for which debug messages are forwarded to the syslog server.

Default Values

By default, debug messages are not sent to the syslog server.

Command History

Release R12.3.0	Command was introduced.

Functional Notes

To receive debug messages through syslog, you must first set the syslog priority to debug, using the command *logging forwarding priority-level on page 1602*.

Usage Examples

The following example specifies that Link Layer Discovery Protocol (LLDP) debug messages are sent to the AOS syslog server:

(config)**#logging forwarding debug lldp**

logging forwarding priority-level

Use the **logging forwarding priority-level** command to set the threshold for events sent to the configured syslog server specified using the command *logging forwarding receiver-ip <ipv4 address> on page 1603*. All events with the specified priority or higher will be sent to all configured syslog servers. Use the **no** form of this command to return to the default priority. Variations of this command include:

logging forwarding priority-level debug
logging forwarding priority-level error
logging forwarding priority-level fatal
logging forwarding priority-level info
logging forwarding priority-level notice
logging forwarding priority-level smdr
logging forwarding priority-level warning

Syntax Description

Sets the minimum priority threshold for sending messages to the syslog server specified using the **logging forwarding receiver-ip** command. The following priorities are available (ranking from lowest to highest):

debug	Logs subsystem debugging events.
error	Logs events with **error** and **fatal** priorities.
fatal	Logs only events with a **fatal** priority.
info	Logs all events.
notice	Logs events with **notice**, **warning**, **error**, and **fatal** priorities.
smdr	Logs events with **smdr** priorities.
warning	Logs events with **warning**, **error**, and **fatal** priorities.

Default Values

By default, the **logging forwarding priority-level** is set to **warning**.

Command History

Release 1.1	Command was introduced.
Release 12.1	Command was expanded to include the **smdr** parameter.
Release R10.1.0	Command was expanded to include the **debug** keyword.

Usage Examples

The following example sends all messages with **warning** level or greater to the syslog server listed using the **logging forwarding receiver-ip** command:

(config)**#logging forwarding priority-level warning**

logging forwarding receiver-ip *<ipv4 address>*

Use the **logging forwarding receiver-ip** command to specify the IPv4 address of the syslog server to use when logging events that match the criteria configured using the command *logging forwarding priority-level on page 1602*. Enter this command multiple times to develop a list of syslog servers to use. This command can be applied to the default virtual private network (VPN) routing and forwarding (VRF) instance or a specific VRF instance. Use the **no** form of this command to remove the entry. Variations of this command include:

logging forwarding receiver-ip *<ipv4 address>*
logging forwarding vrf *<name>* **receiver-ip** *<ipv4 address>*

Syntax Description

<ipv4 address>	Specifies the IPv4 address of the syslog server to use when logging messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrf *<name>*	Optional. Specifies a nondefault VRF instance on which the syslog server is located. If no VRF instance is specified, the default unnamed VRF instance is assumed.

Default Values

By default, there are no configured syslog server addresses.

Command History

Release 1.1	Command was introduced.
Release R11.4.0	Command was expanded to include the **vrf** parameter.

Usage Examples

The following example specifies a syslog server (with address **172.5.67.99**) to use when logging messages:

(config)#**logging forwarding receiver-ip 172.5.67.99**

logging forwarding source-interface <*interface*>

Use the **logging forwarding source-interface** command to configure the specified interface's for the syslog server to use when logging events. This command can be applied to the default virtual private network (VPN) routing and forwarding (VRF) instance or a specific VRF instance. Use the **no** form of this command to remove the source-interface. Variations of this command include:

logging forwarding source-interface <*interface*>
logging forwarding vrf <*name*> **source-interface** <*interface*>

Syntax Description

<*interface*>	Specifies the interface to be used as the source for event log traffic. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **logging forwarding source-interface?** for a complete list of valid interfaces.
vrf <*name*>	Optional. Specifies a nondefault VRF instance on which the syslog server is located. If no VRF instance is specified, the default unnamed VRF instance is assumed.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R11.4.0	Command was expanded to include the **vrf** parameter.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets through firewalls that would normally be blocked.

Usage Examples

Configures the unit to use the **loopback 1** interface as the source interface for event log traffic:

(config)**#logging forwarding source-interface loopback 1**

mac access-list standard <*name*>

Use the **mac access-list standard** command to create an empty medium access control (MAC) access control list (ACL) and enter the Standard MAC Access List command set. Use the **no** form of this command to delete a MAC ACL and all the entries contained in it. The **mac access-list standard** command is currently for use only with wireless access points (APs). The following lists the complete syntax for the **mac access-list standard** command:

(config)**#mac access-list standard** <*name*>
(config-std-mac-acl)#<*action*> <*source*>

Syntax Description

<*name*>	Identifies the configured MAC ACL using an alphanumeric descriptor. All MAC ACL descriptors are case sensitive.
<*action*>	**permit** Permits entry to the access point for specified wireless station MACs.
<*source*>	Specifies the source used for packet matching. Sources are expressed by using **host** <*mac address*> to specify a single host address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

By default, all AOS security features are disabled and there are no configured MAC ACLs.

Command History

Release 15.1	Command was introduced.

Functional Notes

MAC ACLs are used as packet selectors by the wireless features; by themselves, the MAC ACLs do nothing. A MAC ACL entry contains two parts: an action (**permit**) and a MAC address. A **permit** ACL is used to match packets (meeting the specified pattern) to enter the AP. AOS provides only standard MAC ACLs. Standard ACLs match based on the source of the packet.

Usage Examples

The following example creates a MAC ACL named **Trusted** to permit all packets entry to the AP with MAC address **00:A0:C8:00:00:01**.

(config)**#mac access-list standard Trusted**
(config-std-mac-acl)**#permit 00:A0:C8:00:00:01**

For more information about configuring MAC ACLs, refer to the *MAC ACL* quick configuration guide available online at https://supportcommunity.adtran.com.

mac address-table aging-time <*value*>

Use the **mac address-table aging-time** command to set the length of time dynamic medium access control (MAC) addresses remain in the switch or bridge forwarding table. Use the **no** form of this command to reset this length to the default setting.

Syntax Description

<*value*>	Sets an aging time in seconds. Range is **10** to **1000000** seconds. Set to 0 to disable the timeout.

Default Values

By default, the aging time is **300** seconds.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the aging time to **10** minutes:

(config)**#mac address-table aging-time 600**

mac address-table static *<mac address>*

Use the **mac address-table static** command to insert a static medium access control (MAC) address entry into the MAC address table. Use the **no** form of this command to remove an entry from the table. Variations of this command include:

mac address-table static *<mac address>* **bridge** *<bridge id>* **interface** *<interface>*
mac address-table static *<mac address>* **vlan** *<vlan id>* **interface** *<interface>*

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
bridge *<bridge id>*	Specifies a bridge interface ID. Valid range is 1 to 255.
vlan *<vlan id>*	Specifies a virtual local area network (VLAN) interface ID. Valid range is **1** to **4094**.
interface *<interface>*	Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **mac address-table static bridge interface ?** or **mac address-table static** *<mac address>* **vlan** *<vlan id>* **interface ?** for a complete list of valid interfaces.

Default Values

By default, there are no static entries configured.

Command History

Release 5.1	Command was introduced
Release 10.1	Command was expanded to include the bridge interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example adds a static MAC address to Point-to-Point Protocol (PPP) 1 on bridge 4:

(config)**#mac address-table static 00:A0:C8:00:00:01 bridge 4 interface ppp 1**

The following example adds a static MAC address to Ethernet 0/1 on VLAN 4:

(config)**#mac address-table static 00:A0:C8:00:00:01 00:12:79:00:00:01 vlan 4 interface ethernet 0/1**

mac hw-access-list extended <*name*>

Use the **mac hw-access-list extended** command to create and name a medium access control (MAC) hardware access control list (ACL). This command also enters the ACL's configuration mode. Using the **no** form of this command deletes the MAC hardware ACL.

> NOTE *For a complete list of all MAC hardware ACL configuration commands, refer to the* *Hardware ACL and Access Map Command Set on page 4235*.

Syntax Description

<*name*>	Specifies the name of the MAC hardware ACL.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware ACLs.

Command History

Release 17.6	Command was introduced.

Functional Notes

This command only creates an empty hardware ACL, it does not configure it. For additional MAC hardware ACL configuration commands and configuration parameters, refer to the *Hardware ACL and Access Map Command Set on page 4235* or the *Hardware ACLs in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a MAC hardware ACL **Trusted** and enters the MAC hardware ACL configuration mode:

```
(config)#mac hw-access-list extended Trusted
        Configuring New MAC Hardware Extended ACL "Trusted"
(config-ext-mac-hw-nacl)#
```

Technology Review

Hardware ACLs are used as frame selectors by the hardware access maps; by themselves they do nothing. Hardware ACLs are composed of an ordered list of entries with an implicit **deny any** at the end of each list. A hardware ACL with no entries includes an implicit **permit any**. An ACL entry contains two parts: an action (**permit** or **deny**) and a frame pattern. A **permit** ACL matches frames (meeting the specified pattern) and allows them to enter the router system. A **deny** ACL advances AOS to the next access list entry.

ACL criteria are compared to the incoming frame in the order in which they were entered or from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

mail-client *<agent name>*

Use the **mail-client** command to create a general-purpose mail agent and enter the Mail Agent Configuration mode. Use the **no** form of this command to delete the mail agent. Refer to the *Mail Agent Command Set on page 4423* for more information.

Syntax Description

<agent name>	Specifies the name of the created mail agent.

Default Values

By default, no mail agents exist.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example creates a mail agent called **myagent** and enters the Mail Agent Configuration mode:

```
(config)#mail-client myagent
(config-mail-client-myagent)#
```


mef evc <*name*>

Use the **mef evc** command to create an Ethernet virtual connection (EVC) and enter the EVC configuration mode. Using the **no** form of this command removes the EVC from the AOS unit's configuration.

Syntax Description

<*name*>	Specifies the name for the EVC.

Default Values

By default, no EVCs are configured.

Command History

Release A4.01	Command was introduced.

Functional Notes

The EVC connects two endpoints (for example, an Ethernet in the first mile (EFM) group and the Metro Ethernet Forum (MEF) Ethernet interface) and passes Ethernet service frames though the endpoints. The EVCs prevent data transfer between subscriber sites that are not part of the same EVC, thus providing data privacy and security similar to a Frame Relay or an asynchronous transfer mode (ATM) permanent virtual circuit (PVC). EVCs are configured to be part of a bonding group (EFM group).

More information about the configuration of EVCs can be found in the *MEF EVC Command Set on page 3674* or in the *Configuring EFM NIM2s and the MEF Ethernet Interface in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates an EVC named **DATA** and enters the EVC configuration mode:

```
(config)#mef evc DATA
(config-evc-DATA)#
```


mef evc-map *<name>*

Use the **mef evc-map** command to create a Metro Ethernet Forum (MEF) Ethernet virtual connection (EVC) map and enter the EVC Map Configuration mode. The EVC map is used to match traffic to a specific EVC using matching criteria similar to that of quality of service (QoS) matching. Using the **no** form of this command removes the EVC map from the AOS unit's configuration.

Syntax Description

<name>	Specifies the name of the EVC map.

Default Values

By default, no EVC maps are configured.

Command History

Release A4.01	Command was introduced.

Functional Notes

Once an EVC map is created, it must be configured and applied to both an EVC and a user network interface (UNI). For more information about the configuration of EVC maps, refer to *MEF EVC Map Command Set on page 3678* or the *Configuring EFM NIM2s and the MEF Ethernet Interface in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the EVC map **Map1** and enters the EVC Map Configuration mode:

```
(config)#mef evc-map Map1
(config-evc-map-Map1)#
```


mef policer *<name>*

Use the **mef policer** command to create a Metro Ethernet Forum (MEF) policer policy and enter the MEF Policer Policy Configuration mode. The EVC policer policy limits the amount of traffic outbound from the AOS unit to the Metro Ethernet network (MEN). Using the **no** form of this command removes the MEF policer policy from the AOS unit's configuration.

Syntax Description

<name>	Specifies the name of the MEF policer policy.

Default Values

By default, no MEF policer policies are configured.

Command History

Release A4.01	Command was introduced.

Functional Notes

The EVC policer policy can limit traffic on Ethernet virtual connections (EVCs), user network interfaces (UNIs), or EVC maps based on traffic committed burst size (CBS), committed information rate (CIR), excess burst size (EBS), and excess information rate (EIR). These thresholds are used to determine when the EVC bandwidth usage is too great, and the traffic is either queued or dropped based on the configured thresholds. For more information about the configuration and use of EVC policer policies, refer to *MEF Policer Policy Command Set on page 3684* or the *Configuring EFM NIM2s and the MEF Ethernet Interface in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the MEF policer policy **Policy1** and enters the MEF Policer Policy Configuration mode:

```
(config)#mef policer Policy1
(config-policer-Policy1)#
```


mef qos

Use the **mef qos** command to configure the Metro Ethernet Forum (MEF) Ethernet quality of service (QoS) parameters. These parameters specify the hardware queues used by the Ethernet virtual connection (EVC) when traffic matching an EVC map is discovered, as well as the Metro Ethernet network (MEN) priority given to untagged traffic. Using the **no** form of this command returns the MEF QoS settings to the default values. Variations of this command include:

mef qos cos-map <*number*> <*value*>
mef qos untagged <*value*>

Syntax Description

cos-map <*number*> <*value*>	Specifies default mapping of queues to class of service (CoS) markings for EVC traffic. The <*number*> parameter is the queue to which a CoS value is mapped. Valid range is **1** to **8**. The <*value*> parameter is the CoS value assigned to the queue. Valid value range is **0** to **7**.
untagged <*value*>	Specifies the MEN priority for untagged traffic on the EVC. Valid range is **0** to **7**.

Default Values

By default, a MEN priority of **0** is assigned to untagged traffic.

The default MEF QoS queue assignments are outlined below.

Queue and Assigned CoS Values	One CoS Value Is Assigned to Each Queue by Default
(config)**#mef qos cos-map 1 1**	CoS value 1 is assigned to queue 1 by default.
(config)**#mef qos cos-map 2 0**	CoS value 0 is assigned to queue 2 by default.
(config)**#mef qos cos-map 3 2**	CoS value 2 is assigned to queue 3 by default.
(config)**#mef qos cos-map 4 3**	CoS value 3 is assigned to queue 4 by default.
(config)**#mef qos cos-map 5 4**	CoS value 4 is assigned to queue 5 by default.
(config)**#mef qos cos-map 6 5**	CoS value 5 is assigned to queue 6 by default.
(config)**#mef qos cos-map 7 6**	CoS value 6 is assigned to queue 7 by default.
(config)**#mef qos cos-map 8 7**	CoS value 7 is assigned to queue 8 by default.

Command History

Release A4.01	Command was introduced.

Functional Notes

The MEF QoS CoS map values are used by the EVC map when the MEN queue setting is specified as **inherit**. For more information about the relationships between and configuration of MEF components, refer to the *Configuring EFM NIM2s and the MEF Ethernet Interface in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that traffic with CoS values **3** and **4** are mapped to queue **1**:

(config)**#mef qos cos-map 1 3 4**

The following example specifies the MEN priority for untagged traffic is **5**:

(config)**#mef qos untagged 5**

modem countrycode <*value*>

Use the **modem countrycode** command to specify the modem configuration for the applicable country.

Syntax Description

<*value*>	Specifies the modem configuration for the applicable country. Refer to *Functional Notes* for countrycode values.

Default Values

By default, **modem countrycode** is set to **USA/Canada**.

Command History

Release 10.1	Command was introduced.

Functional Notes

The following country codes are available for modem configuration:

Algeria	- Algeria Modem configuration
Argentina	- Argentina Modem configuration
Australia	- Australia Modem configuration
Austria	- Austria Modem configuration
Bahrain	- Bahrain Modem configuration
Belgium	- Belgium Modem configuration
Bolivia	- Bolivia Modem configuration
Brazil	- Brazil Modem configuration
Chile	- Chile Modem configuration
China	- China Modem configuration
Colombia	- Colombia Modem configuration
Costa_Rica	- Costa_Rica Modem configuration
Cyprus	- Cyprus Modem configuration
Czechoslovakia	- Czechoslovakia Modem configuration
Denmark	- Denmark Modem configuration
Ecuador	- Ecuador Modem configuration
Egypt	- Egypt Modem configuration
Finland	- Finland Modem configuration
France	- France Modem configuration
Germany	- Germany Modem configuration
Greece	- Greece Modem configuration
Guatemala	- Guatemala Modem configuration
Hong_Kong	- Hong_Kong Modem configuration
Hungary	- Hungary Modem configuration
India	- India Modem configuration
Indonesia	- Indonesia Modem configuration
Ireland	- Ireland Modem configuration
Israel	- Israel Modem configuration

Italy	- Italy Modem configuration
Japan	- Japan Modem configuration
Jordan	- Jordan Modem configuration
Korea	- Korea Modem configuration
Kuwait	- Kuwait Modem configuration
Lebanon	- Lebanon Modem configuration
Malaysia	- Malaysia Modem configuration
Mexico	- Mexico Modem configuration
Morocco	- Morocco Modem configuration
Netherlands	- Netherlands Modem configuration
New_Zealand	- New_Zealand Modem configuration
Norway	- Norway Modem configuration
Oman	- Oman Modem configuration
Panama	- Panama Modem configuration
Peru	- Peru Modem configuration
Philippines	- Philippines Modem configuration
Poland	- Poland Modem configuration
Portugal	- Portugal Modem configuration
Puerto_Rico	- Puerto_Rico Modem configuration
Qatar	- Qatar Modem configuration
Russia	- Russia Modem configuration
Saudi_Arabia	- Saudi_Arabia Modem configuration
Singapore	- Singapore Modem configuration
Slovakia	- Slovakia Modem configuration
Slovenia	- Slovenia Modem configuration
South_Africa	- South_Africa Modem configuration
Spain	- Spain Modem configuration
Sweden	- Sweden Modem configuration
Switzerland	- Switzerland Modem configuration
Syria	- Syria Modem configuration
Taiwan	- Taiwan Modem configuration
Thailand	- Thailand Modem configuration
Trinidad	- Trinidad Modem configuration
Tunisia	- Tunisia Modem configuration
Turkey	- Turkey Modem configuration
UAE	- UAE Modem configuration
UK	- UK Modem configuration
USA/Canada	- USA/Canada Modem configuration
Uruguay	- Uruguay Modem configuration
Venezuela	- Venezuela Modem configuration
Yemen	- Yemen Modem configuration

Usage Examples

The following example specifies to use the **USA/Canada** modem configuration.

(config)**#modem countrycode USA/Canada**

monitor session <*number*>

Use the **monitor session** command to configure a port mirroring session. Use the **no** form of this command to remove a port mirroring session or to remove a source or destination interface. Variations of this command include:

monitor session <*number*> **destination interface** <*interface*> **no-isolate**
monitor session <*number*> **destination interface** <*interface*> **no-tag**
monitor session <*number*> **destination interface** <*interface*> **no-isolate no-tag**
monitor session <*number*> **destination interface** <*interface*> **no-tag no-isolate**
monitor session <*number*> **source interface** <*interface*>
monitor session <*number*> **source interface** <*interface*> **both**
monitor session <*number*> **source interface** <*interface*> **rx**
monitor session <*number*> **source interface** <*interface*> **tx**

Syntax Description

<*number*>	Selects the monitor session number (only one is allowed).
destination	Selects the destination interface.
source	Selects the source interface(s). A range of interfaces is allowed.
interface <*interface*>	Specifies an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **monitor session** <*number*> **[destination	source] interface ?** for a complete list of valid interfaces.
both	Optional. Monitors both transmitted and received traffic.
rx	Optional. Monitors received traffic only.
tx	Optional. Monitors transmitted traffic only.
no-tag	Removes the virtual local area network (VLAN) tag that is normally appended to mirrored traffic.
no-isolate	Allows native traffic to continue to pass on the port set as the mirroring session destination.

Default Values

By default, traffic is monitored in both directions. Also by default, the destination port is isolated from passing native traffic.

Command History

Release 5.1	Command was introduced.
Release 13.1	Command was expanded to include the **no-isolate** parameter.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Usage Examples

The following example sets Ethernet 0/1 as the destination interface and adds Ethernet 0/2, Ethernet 0/3, and Ethernet 0/5 as source ports:

(config)**#monitor session 1 destination interface eth 0/1**
(config)**#monitor session 1 source interface eth 0/2-3, eth 0/5**

The following example sets gigabit switchport 0/1 as the destination interface and removes the VLAN tag:

(config)**#monitor session 1 destination interface gigabit-switchport 0/1 no-tag**

The following example sets switchport 0/1 as the source interface and monitors both transmitted and received traffic:

(config)**#monitor session 1 source interface switchport 0/1 both**

The following example sets gigabit switchport 0/1, and switchport 0/2 through switchport 0/12 as source interfaces and monitors only received traffic:

(config)**#monitor session 1 source interface gigabit 0/1, eth 0/2-12 rx**

name-server

Use the **name-server** command to designate an address for one or more name servers to use for name-to-address domain naming server (DNS) resolution. This command can be applied to the default virtual private network (VPN) routing and forwarding (VRF) instance or a specific VRF instance. Use the **no** form of this command to remove an address. Variations of this command include:

name-server <*ipv4 address*>
name-server <*ipv6 address*>
name-server vrf <*name*> <*ipv4 address*>
name-server vrf <*name*> <*ipv6 address*>

Syntax Description

<*ipv4 address*>	Specifies an Internet Protocol version 4 (IPv4) name server address. IPv4 addresses should be specified in dotted decimal notation (for example, **10.10.10.1**).
<*ipv6 address*>	Specifies an Internet Protocol version 6 (IPv6) name server address. IPv6 address should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
vrf <*name*>	Optional. Specifies a nondefault VRF instance on which to add a name server address. If no VRF instance is specified, the name server is added on the default unnamed VRF instance.

Default Values

By default, no name servers are specified.

Command History

Release 3.1	Command was introduced.
Release 16.1	Command was expanded to include the **vrf** parameter.
Release 18.3	Command was expanded to include IPv6 support for Adtran internetworking products.
Release R10.1.0	Command was expanded to include IPv6 support for Adtran voice products.

Functional Notes

The addition of the server address occurs at the end of the IPv4 or IPv6 addresses in the server list. There is no limit to the number of name server addresses that can be entered. Addresses added using this command are combined with those learned dynamically, and if an IPv6 DNS name server is added, its address is combined with those configured using IPv4 DNS.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example specifies IPv4 host **172.34.1.111** as the primary name server and IPv4 host **172.34.1.2** as the secondary server:

(config)**#name-server 172.34.1.111 172.34.1.2**

network-forensics ip dhcp

Use the **network-forensics ip dhcp** command to enable passive monitoring of Dynamic Host Configuration Protocol (DHCP) message exchanges between the server and the client. Using the **no** form of this command disables network forensics.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 17.8	Command was introduced.

Functional Notes

Network forensics is an AOS feature that collects client information through DHCP messages sent between clients connected to the network and the network server.

Once network forensics is enabled, the AOS unit begins collecting DHCP information. The collected data can be viewed either by using the command *show name-server on page 878* or *debug network-forensics ip dhcp on page 422* to view the information in realtime. For more information about network forensics, refer to the *Network Forensics in AOS* troubleshooting guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables the network forensics feature:

(config)**#network-forensics ip dhcp**

network-sync

Use the **network-sync** command to enable network synchronization (Network Sync) configuration and enter the Network Sync Configuration mode. Use the **no** form of this command to remove Network Sync configuration from the unit.

Syntax Description

No subcommands.

Default Values

By default, Network Sync is disabled.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example enables Network Sync and enters the Network Sync Configuration mode:

```
(config)#network-sync
(config-ntwk-sync)#
```

no activchassis

Use the **no activchassis** command to disable ActivChassis and return the AOS device to a standalone device.

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Command History

Release AC1.0	Command was introduced.

Functional Notes

Devices that are currently ActivChassis members can be restarted in standalone mode. To restart a device in standalone mode, you must first disconnect the device from all other ActivChassis-enabled devices and reboot the unit. The device attempts (and fails) to detect an ActivChassis, and successfully boots as a standalone device. Once the device is disconnected from ActivChassis, and has been rebooted as a standalone device, enter this command from the device's local console. You must confirm that you want the device configuration and mode to be altered. By confirming the action, the local manifest is updated with indications that ActivChassis mode should be disabled at device boot. The startup configuration file is backed up and then deleted, causing the configuration to return to default at the next boot. The device is then rebooted and is in standalone mode.

This command is available from both the ActivChassis master and linecard devices' CLI. For more information about the difference between linecard and master devices, how to access the CLI for each, and additional configuration information, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables ActivChassis and returns the device to standalone mode (after it has been disconnected from the ActivChassis):

(config)**#no activchassis**

ntp ip access-class <*ipv4 acl*> in

Use the **ntp ip access-class** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to incoming connections on the IPv4 Network Time Protocol (NTP) server. Use the **no** form of this command to remove the ACL from the NTP server. Variations of this command include:

ntp ip access-class <*ipv4 acl*> **in**
ntp ip access-class <*ipv4 acl*> **in any-vrf**
ntp ip access-class <*ipv4 acl*> **in vrf** <*name*>

Syntax Description

<*ipv4 acl*>	Specifies the IPv4 ACL to apply to the IPv4 NTP server.
in	Specifies that the ACL is applied to incoming connections.
any-vrf	Optional. Specifies that incoming connections from any virtual routing and forwarding (VRF) instance are allowed.
vrf <*name*>	Optional. Specifies that incoming connections from the specified nondefault VRF instance are allowed. If no VRF is specified, incoming connections only from the default unnamed VRF instance are allowed.

Default Values

By default, no ACLs are applied to the NTP server.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example applies the IPv4 ACL **MYIPV4ACL** to incoming connections on the default VRF instance to the IPv4 NTP server:

(config)**#ntp ip access-class MYIPV4ACL in**

ntp ipv6 access-class <*ipv6 acl*> in

Use the **ntp ipv6 access-class** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to incoming connections on the IPv6 Network Time Protocol (NTP) server. Use the **no** form of this command to remove the ACL from the NTP server. Variations of this command include:

ntp ipv6 access-class <*ipv6 acl*> **in**
ntp ipv6 access-class <*ipv6 acl*> **in any-vrf**
ntp ipv6 access-class <*ipv6 acl*> **in vrf** <*name*>

Syntax Description

<*ipv6 acl*>	Specifies the IPv6 ACL to apply to the IPv6 NTP server.
in	Specifies that the ACL is applied to incoming connections.
any-vrf	Optional. Specifies that incoming connections from any virtual routing and forwarding (VRF) instance are allowed.
vrf <*name*>	Optional. Specifies that incoming connections from the specified nondefault VRF instance are allowed. If no VRF is specified, incoming connections only from the default unnamed VRF instance are allowed.

Default Values

By default, no ACLs are applied to the NTP server.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example applies the IPv6 ACL **MYIPV6ACL** to incoming connections on the default VRF instance to the IPv6 NTP server:

(config)**#ntp ipv6 access-class MYIPV6ACL in**

ntp master

Use the **ntp master** command to globally set the system as an authoritative Network Time Protocol (NTP) server. Variations of this command include:

ntp master
ntp master <*value*>

Syntax Description

<*value*>	Optional. Specify the stratum number. The valid range is **1** to **15**. We recommend not setting the stratum higher than **2**.

Default Values

By default, the NTP server is not enabled.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example enables the master NTP server:

(config)**#ntp master**

ntp max-associations <*value*>

Use the **ntp max-associations** command to set the maximum number of simultaneous Network Time Protocol (NTP) associations allowed with other NTP clients or peers. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specify the maximum number of associations. The valid range is **1** to **4294967295**.

Default Values

By default, the maximum associations is **100**.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example specifies the maximum associations of **250**:

(config)**#ntp max-associations 250**

ntp peer <*hostname* | *ipv4 address*>

Use the **ntp peer** command to specify an Internet Protocol version 4 (IPv4) peer association with another Network Time Protocol (NTP) system and configure its parameters. Any combination of peer associations can be simultaneously configured. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the association to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the association to the default unnamed VRF. Use the **no** form of this command to return to the default setting. Variations of this command include:

ntp peer <*hostname* | *ipv4 address*>
ntp peer <*hostname* | *ipv4 address*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **minpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **normal-sync**
ntp peer <*hostname* | *ipv4 address*> **prefer**
ntp peer <*hostname* | *ipv4 address*> **source** <*interface*>
ntp peer <*hostname* | *ipv4 address*> **version**

ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **minpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **normal-sync**
ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **prefer**
ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*>
ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version**
ntp peer <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version maxpoll** <*value*>

ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*>
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **minpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **normal-sync**
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **prefer**
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*>
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version**
ntp peer <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version maxpoll** <*value*>

ntp peer <*hostname* | *ipv4 address*> **system-control-evc**
ntp peer <*hostname* | *ipv4 address*> **system-control-evc maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **system-control-evc minpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **system-control-evc normal-sync**
ntp peer <*hostname* | *ipv4 address*> **system-control-evc prefer**
ntp peer <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*>
ntp peer <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **system-control-evc version**
ntp peer <*hostname* | *ipv4 address*> **system-control-evc version maxpoll** <*value*>

ntp peer <*hostname* | *ipv4 address*> **system-management-evc**

ntp peer <*hostname* | *ipv4 address*> **system-management-evc maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **system-management-evc minpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **system-management-evc normal-sync**
ntp peer <*hostname* | *ipv4 address*> **system-management-evc prefer**
ntp peer <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*>
ntp peer <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv4 address*> **system-management-evc version**
ntp peer <*hostname* | *ipv4 address*> **system-management-evc version maxpoll** <*value*>

ntp peer vrf <*name*> <*hostname* | *ipv4 address*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **prefer**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **version**

ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **prefer**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version maxpoll** <*value*>

ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **prefer**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version maxpoll** <*value*>

ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc prefer**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*>

maxpoll <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc version**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc version maxpoll** <*value*>

ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc prefer**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc version**
ntp peer vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc version maxpoll** <*value*>

Syntax Description

<*hostname* | *ipv4 address*>	Specify the host name or IPv4 address of the NTP server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
efm-group <*group id*>	Specifies an Ethernet in the first mile (EFM) group ID. Range is **1** to **1024**.
maxpoll <*value*>	Optional. Specifies the maximum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the **maxpoll** to 10 would indicate a maximum polling interval of **1024** seconds. Refer to the fuctional notes of this command for more information.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
minpoll <*value*>	Optional. Specifies the minimum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the **minpoll** to 6 would indicate a minimum polling interval of **64** seconds. Refer to the *Functional Notes* for more information.
normal-sync	Optional. Disables the rapid synchronization feature.
prefer	Optional. Specifies the preference of using the specified server above all other configured NTP servers.
source <*interface*>	Optional. Specifies the source interface (physical or virtual) to use for the peer. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **ntp peer** <*name*> **source ?** for a list of valid interfaces.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC exists by default and cannot be deleted.
system-management-evc	Specifies the system management EVC. This EVC exists by default and cannot be deleted.
version	Specifies the version number for outgoing NTP packets. Valid range is **2** to **4**.

vrf <*name*>	Specifies the name of the VRF to which to assign the association. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, the **ntp peer** is not set. Once enabled, the default version is **4**, the default **minpoll** interval is **6** (64 seconds) and the default **maxpoll** interval is **10** (1024 seconds).

Command History

Release 17.2	Command was introduced.
Release 17.6	Command was expanded to include **maxpoll** and **minpoll** parameters.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.1.0	Command was expanded to include the bridged virtual interface (BVI).
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R11.2.0	Command was expanded to include Ethernet in the first mile (EFM) group parameter.
Release R13.7.0	Command was expanded to include the virtual local area network (VLAN) interface.

Functional Notes

The IPv4 **ntp peer** command can be executed with any combination of the following parameters:

maxpoll <*value*>
minpoll <*value*>
normal-sync
prefer
source <*interface*>
version

For example, the **normal-sync** and **source** <*interface*> parameters can be used in conjunction with one another. In this case, the command would look like this:

#ntp peer 10.10.10.1 normal-sync source ppp 1

These parameters can be combined in any order to obtain the desired configuration.

In order to determine the appropriate value to enter for **maxpoll** or **minpoll**, use the following formula: 2^n where n = <*value*>. For example, to set the minimum polling interval to 64 seconds, you would enter **6** as the **minpoll** value. This corresponds to 2^6 in the formula, or 2x2x2x2x2x2, which equals 64 seconds.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example defines **10.10.10.1** as the IPv4 NTP peer:

(config)**#ntp peer 10.10.10.1**

The following example creates an IPv4 peer association with **10.10.10.1** and sets the maximum polling interval of 64 seconds:

(config)**#ntp peer** 10.10.10.1 **maxpoll 6**

ntp peer <*hostname* | *ipv6 address*>

Use the **ntp peer** command to enable Network Time Protocol (NTP), and specify an Internet Protocol version 6 (IPv6) peer association with another NTP system and configure the association's parameters. Any combination of peer associations can be simultaneously configured. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the association to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the association to the default unnamed VRF. Use the **no** form of this command to return to the default setting. Variations of this command include:

ntp peer <*hostname* | *ipv6 address*>
ntp peer <*hostname* | *ipv6 address*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **minpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **normal-sync**
ntp peer <*hostname* | *ipv6 address*> **prefer**
ntp peer <*hostname* | *ipv6 address*> **source** <*interface*>
ntp peer <*hostname* | *ipv6 address*> **version**

ntp peer <*hostname* | *ipv6 address*> <*interface*>
ntp peer <*hostname* | *ipv6 address*> <*interface*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> <*interface*> **minpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> <*interface*> **normal-sync**
ntp peer <*hostname* | *ipv6 address*> <*interface*> **prefer**
ntp peer <*hostname* | *ipv6 address*> <*interface*> **source** <*interface*>
ntp peer <*hostname* | *ipv6 address*> <*interface*> **version**

ntp peer <*hostname* | *ipv6 address*> **system-control-evc**
ntp peer <*hostname* | *ipv6 address*> **system-control-evc maxpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **system-control-evc minpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **system-control-evc normal-sync**
ntp peer <*hostname* | *ipv6 address*> **system-control-evc prefer**
ntp peer <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*>
ntp peer <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **system-control-evc version**
ntp peer <*hostname* | *ipv6 address*> **system-control-evc version maxpoll** <*value*>

ntp peer <*hostname* | *ipv6 address*> **system-management-evc**
ntp peer <*hostname* | *ipv6 address*> **system-management-evc maxpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **system-management-evc minpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **system-management-evc normal-sync**
ntp peer <*hostname* | *ipv6 address*> **system-management-evc prefer**
ntp peer <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*>
ntp peer <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp peer <*hostname* | *ipv6 address*> **system-management-evc version**
ntp peer <*hostname* | *ipv6 address*> **system-management-evc version maxpoll** <*value*>

ntp peer vrf <*name*> <*hostname* | *ipv6 address*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **maxpoll** <*value*>

ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **prefer**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **version**

ntp peer vrf <*name*> <*hostname* | *ipv6 address*> <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **prefer**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **version**

ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc prefer**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc version**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc version maxpoll** <*value*>

ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc minpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc normal-sync**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc prefer**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc version**
ntp peer vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc version maxpoll** <*value*>

Syntax Description

<*hostname* | *ipv6 address*>	Specify the host name or IPv6 address of the NTP server. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

<interface>	Specifies which interface NTP should use to send NTP requests. This option is only available when a link-local IPv6 address is used for the NTP peer, and it must be specified. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **ntp peer** *<name>* **source ?** for a list of valid interfaces.
maxpoll *<value>*	Optional. Specifies the maximum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the **maxpoll** to 10 would indicate a maximum polling interval of **1024** seconds. Refer to the the *Functional Notes* for more information.
minpoll *<value>*	Optional. Specifies the minimum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the **minpoll** to 6 would indicate a minimum polling interval of **64** seconds. Refer to the the *Functional Notes* for more information.
normal-sync	Optional. Disables the rapid synchronization feature.
prefer	Optional. Specifies the preference of using the specified peer above all other configured NTP servers.
source *<interface>*	Optional. Specifies the source interface (physical or virtual) to use for the peer. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **ntp peer** *<name>* **source ?** for a list of valid interfaces.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC exists by default and cannot be deleted.
system-management-evc	Specifies the system management EVC. This EVC exists by default and cannot be deleted.
version	Specifies the version number for outgoing NTP packets. Valid range is **2** to **4**.
vrf *<name>*	Specifies the name of the VRF to which to assign the association. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, the IPv6 **ntp peer** is not set. Once enabled, the default version is **4**, the default **minpoll** interval is **6** (64 seconds) and the default **maxpoll** interval is **10** (1024 seconds).

Command History

Release R10.3.0	Command was introduced.
Release R10.7.0	Command was expanded to include the **vrf** *<name>* parameter.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.

Release R13.7.0	Command was expanded to include the Gigabit Ethernet and virtual loacl area network (VLAN) interfaces.

Functional Notes

The IPv6 **ntp peer** command can be executed with any combination of the following parameters:

maxpoll <*value*>
minpoll <*value*>
normal-sync
prefer
source <*interface*>
version

For example, the **normal-sync** and **source** <*interface*> parameters can be used in conjunction with one another. In this case, the command would look like this:

#ntp peer fe80::2 vlan 1 normal-sync source ppp 1

These parameters can be combined in any order to obtain the desired configuration.

In order to determine the appropriate value to enter for **maxpoll** or **minpoll**, use the following formula: 2^n where n = <*value*>. For example, to set the minimum polling interval to 64 seconds, you would enter **6** as the **minpoll** value. This corresponds to 2^6 in the formula, or 2x2x2x2x2x2, which equals 64 seconds.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example defines **fe80::2 vlan 1** as the IPv6 NTP peer:

(config)**#ntp peer fe80::2 vlan 1**

The following example creates an IPv6 peer association with **2001:DB8:1::1** and sets the maximum polling interval of 64 seconds:

(config)**#ntp peer 2001:DB8:1::1 maxpoll 6**

ntp server <*hostname* | *ipv4 address*>

Use the **ntp server** command to specify an Internet Protocol version 4 (IPv4) server association with another Network Time Protocol (NTP) system and configure its parameters. Any combination of server associations can be simultaneously configured. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the association to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the association to the default unnamed VRF. Use the **no** form of this command to return to the default setting. Variations of this command include:

ntp server <*hostname* | *ipv4 address*>
ntp server <*hostname* | *ipv4 address*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **minpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **prefer**
ntp server <*hostname* | *ipv4 address*> **source** <*interface*>
ntp server <*hostname* | *ipv4 address*> **version** <*number*>

ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*>
ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*> **minpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*> **prefer**
ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*>
ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version**
ntp server <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version maxpoll** <*value*>

ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*>
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **minpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **normal-sync**
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **prefer**
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*>
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version**
ntp server <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version maxpoll** <*value*>

ntp server <*hostname* | *ipv4 address*> **system-control-evc**
ntp server <*hostname* | *ipv4 address*> **system-control-evc maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **system-control-evc minpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **system-control-evc normal-sync**
ntp server <*hostname* | *ipv4 address*> **system-control-evc prefer**
ntp server <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*>
ntp server <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **system-control-evc version**
ntp server <*hostname* | *ipv4 address*> **system-control-evc version maxpoll** <*value*>

ntp server <*hostname* | *ipv4 address*> **system-management-evc**
ntp server <*hostname* | *ipv4 address*> **system-management-evc maxpoll** <*value*>

ntp server <*hostname* | *ipv4 address*> **system-management-evc minpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **system-management-evc prefer**
ntp server <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*>
ntp server <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv4 address*> **system-management-evc version**
ntp server <*hostname* | *ipv4 address*> **system-management-evc version maxpoll** <*value*>

ntp server vrf <*name*> <*hostname* | *ipv4 address*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **prefer**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **version** <*number*>

ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **prefer**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **source** <*interface*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version** <*number*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **efm-group** <*group id*> **version** <*number*> **maxpoll** <*value*>

ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **prefer**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **source** <*interface*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **mef-ethernet** <*slot/port*> **version maxpoll** <*value*>

ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc prefer**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc source** <*interface*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc version**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-control-evc version maxpoll** <*value*>

ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc**

ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc prefer**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc version**
ntp server vrf <*name*> <*hostname* | *ipv4 address*> **system-management-evc version maxpoll** <*value*>

Syntax Description

<*hostname* | *ipv4 address*>	Specify the host name or IPv4 address of the NTP server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
efm-group <*group id*>	Specifies an Ethernet in the first mile (EFM) group ID. Range is **1** to **1024**.
maxpoll <*value*>	Optional. Specifies the maximum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the maxpoll to 10 would indicate a maximum polling interval of **1024** seconds. Refer to the the *Functional Notes* for more information.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
minpoll <*value*>	Optional. Specifies the minimum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the minpoll to 6 would indicate a minimum polling interval of **64** seconds. Refer to the the *Functional Notes* for more information.
prefer	Optional. Specifies the preference of using the specified server above all other configured NTP servers.
source <*interface*>	Optional. Specifies the source interface (physical or virtual) to use for the server. Specify an interface in the format <*interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Enter **ntp server** <*name*> **source ?** for a list of valid interfaces.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC exists by default and cannot be deleted.
system-management-evc	Specifies the system management EVC. This EVC exists by default and cannot be deleted.
version <*number*>	Specifies the version number for outgoing NTP packets. Valid range is **2** to **4**.
vrf <*name*>	Specifies the name of the VRF to which to assign the association. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, the IPv6 **ntp server** is not set. Once enabled, the default version is **4**, the default **minpoll** interval is **6** (64 seconds) and the default **maxpoll** interval is **10** (1024 seconds).

Command History

Release 17.2	Command was introduced.
Release 17.6	Command was expanded to include **maxpoll** and **minpoll** parameters.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.1.0	Command was expanded to include the bridged virtual interface (BVI).
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R11.2.0	Command was expanded to include Ethernet in the first mile (EFM) group parameter.

Functional Notes

The IPv4 **ntp server** command can be executed with any combination of the following parameters:

maxpoll <*value*>
minpoll <*value*>
prefer
source <*interface*>
version

For example, the **prefer** and **source** <*interface*> parameters can be used in conjunction with one another. In this case, the command would look like this:

#ntp server 10.10.10.1 prefer source ppp 1

These parameters can be combined in any order to obtain the desired configuration.

In order to determine the appropriate value to enter for **maxpoll** or **minpoll**, use the following formula: 2^n where n = <*value*>. For example, to set the minimum polling interval to 64 seconds, you would enter **6** as the **minpoll** value. This corresponds to 2^6 in the formula, or 2x2x2x2x2x2, which equals 64 seconds.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example defines **10.10.10.1** as the preferred IPv4 NTP server:

(config)**#ntp server 10.10.10.1 prefer**

The following example associates the IPv4 NTP server **10.10.10.1** and sets the minimum polling interval of 256 seconds:

(config)**#ntp server 10.10.10.1 maxpoll 8**

ntp server <*hostname* | *ipv6 address*>

Use the **ntp server** command to specify an Internet Protocol version 6 (IPv6) server association with another Network Time Protocol (NTP) system and configure the association's parameters. Any combination of server associations can be simultaneously configured. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the association to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the association to the default unnamed VRF. Use the **no** form of this command to return to the default setting. Variations of this command include:

ntp server <*hostname* | *ipv6 address*>
ntp server <*hostname* | *ipv6 address*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **minpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **prefer**
ntp server <*hostname* | *ipv6 address*> **source** <*interface*>
ntp server <*hostname* | *ipv6 address*> **version** <*number*>

ntp server <*hostname* | *ipv6 address*> **system-control-evc**
ntp server <*hostname* | *ipv6 address*> **system-control-evc maxpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **system-control-evc minpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **system-control-evc normal-sync**
ntp server <*hostname* | *ipv6 address*> **system-control-evc prefer**
ntp server <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*>
ntp server <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **system-control-evc version**
ntp server <*hostname* | *ipv6 address*> **system-control-evc version maxpoll** <*value*>

ntp server <*hostname* | *ipv6 address*> **system-management-evc**
ntp server <*hostname* | *ipv6 address*> **system-management-evc maxpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **system-management-evc minpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **system-management-evc prefer**
ntp server <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*>
ntp server <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> **system-management-evc version**
ntp server <*hostname* | *ipv6 address*> **system-management-evc version maxpoll** <*value*>

ntp server <*hostname* | *ipv6 address*> <*interface*>
ntp server <*hostname* | *ipv6 address*> <*interface*> **maxpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> <*interface*> **minpoll** <*value*>
ntp server <*hostname* | *ipv6 address*> <*interface*> **prefer**
ntp server <*hostname* | *ipv6 address*> <*interface*> **source** <*interface*>
ntp server <*hostname* | *ipv6 address*> <*interface*> **version** <*number*>

ntp server vrf <*name*> <*hostname* | *ipv6 address*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **prefer**
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **source** <*interface*>

ntp server vrf <*name*> <*hostname* | *ipv6 address*> **version** <*number*>

ntp server vrf <*name*> <*hostname* | *ipv6 address*> <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **prefer**
ntp server vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> <*interface*> **version** <*number*>

ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc**
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc prefer**
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc source** <*interface*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc version**
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-control-evc version maxpoll** <*value*>

ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc**
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc minpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc prefer**
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc source** <*interface*> **maxpoll** <*value*>
ntp server vrf <*name*> <*hostname* | *ipv6 address*> **system-management-evc version**

Syntax Description

<*hostname* | *ipv6 address*>	Specify the host name or IPv6 address of the NTP server. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*interface*>	Specifies which interface NTP should use to send NTP requests. This option is only available when a link-local IPv6 address is used for the NTP peer, and it must be specified. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **ntp peer** <*name*> **source ?** for a list of valid interfaces.
maxpoll <*value*>	Optional. Specifies the maximum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the maxpoll to 10 would indicate a maximum polling interval of **1024** seconds. Refer to the the *Functional Notes* for more information.

minpoll <*value*>	Optional. Specifies the minimum polling interval for NTP packets, in seconds as a power of two. The allowable range is **4** to **17**. For example, setting the minpoll to 6 would indicate a minimum polling interval of **64** seconds. Refer to the the *Functional Notes* for more information.
prefer	Optional. Specifies the preference of using the specified server above all other configured NTP servers.
source <*interface*>	Optional. Specifies the source interface (physical or virtual) to use for the server. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Enter **ntp server** <*name*> **source ?** for a list of valid interfaces.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC). This EVC exists by default and cannot be deleted.
system-management-evc	Specifies the system management EVC. This EVC exists by default and cannot be deleted.
version <*number*>	Specifies the version number for outgoing NTP packets. Valid range is **2** to **4**.
vrf <*name*>	Specifies the name of the VRF to which to assign the association. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, the **ntp server** is not set. Once enabled, the default version is **4**, the default **minpoll** interval is **6** (64 seconds) and the default **maxpoll** interval is **10** (1024 seconds).

Command History

Release R10.3.0	Command was introduced.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** parameters.

Functional Notes

The IPv6 **ntp server** command can be executed with any combination of the following parameters:

maxpoll <*value*>
minpoll <*value*>
prefer
source <*interface*>
version

For example, the **prefer** and **source** <*interface*> parameters can be used in conjunction with one another. In this case, the command would look like this:

#ntp server 10.10.10.1 prefer source ppp 1

These parameters can be combined in any order to obtain the desired configuration.

In order to determine the appropriate value to enter for **maxpoll** or **minpoll**, use the following formula: 2^n where n = <*value*>. For example, to set the minimum polling interval to 64 seconds, you would enter **6** as the **minpoll** value. This corresponds to 2^6 in the formula, or 2x2x2x2x2x2, which equals 64 seconds.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example defines **fe80::2 vlan 1** as the preferred IPv6 NTP server:

(config)**#ntp server fe80::2 vlan 1 prefer**

The following example associates the IPv6 NTP server **2001:DB8:1::1** and sets the minimum polling interval of 256 seconds:

(config)**#ntp server 2001:DB8:1::1 maxpoll 8**

ntp source *<interface>*

Use the **ntp source** command to specify the source interface for the Network Time Protocol (NTP) packets. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the association to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the association to the default unnamed VRF. Use the **no** form of this command to return to the default setting. Variations of this command include:

ntp source <*interface*>
ntp vrf <*name*> **source** <*interface*>

Syntax Description

<interface>	Specifies the source interface (physical or virtual) to use for the server. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Enter **ntp source ?** for a list of valid interfaces.
vrf <*name*>	Specifies the name of the VRF to which to assign the association. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, the NTP source interface is not set.

Command History

Release 17.2	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example defines NTP source interface as **ppp 1**:

(config)**#ntp source ppp 1**

ntp update-rtc

Use the **ntp update-rtc** command to specify periodically updating the clock in real time. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the Network Time Protocol (NTP) is disabled.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example sets the clock to periodically update the timing:

(config)**#ntp update-rtc**

over-temperature protection

Use the **over-temperature protection** command to enter the Over-Temperature Protection Configuration mode, from which to configure the over temperature protection feature. Additional commands are available for configuring this feature and are explained in *Over-Temperature Protection Command Set on page 4446*.

Syntax Description

No subcommands.

Default Values

By default, the over-temperature protection mode is disabled.

Command History

Release R11.6.0	Command was introduced.

Functional Notes

For more information regarding over-temperature protection configuration, refer to the *Over-Temperature Protection Command Set on page 4446*.

Usage Examples

The following example enters the Over-Temperature Protection Configuration mode:

```
(config)#over-temperature protection
(config-over-temp-protection)#
```


packet-capture <*name*>

Use the **packet-capture** command to create a packet-capture on the AOS device and enter the packet-capture's configuration mode. Packet-captures are used with network monitoring on interfaces to effectively capture data packets as they traverse the network. Use the **no** form of this command to remove the packet-capture. Variations of this command include:

packet-capture <*name*> **standard**
packet-capture <*name*> **sip**

Syntax Description

<*name*>	Specifies the name of the packet-capture. Names can be between **1** and **32** characters in length.
standard	Specifies that all ingress and egress Internet Protocol version 4 (IPv4) packets are captured.
sip	Specifies that all ingress and egress User Datagram Protocol (UDP) packets that are related to Session Initiation Protocol (SIP) messages are captured.

Default Values

By default, no packet-captures are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. As data packets pass through an interface on which the packet capturing feature is enabled, a packet-capture monitors the traffic and captures the header and payload of specified packets as they pass through. The captured packets are then exported and stored in either flash memory or CompactFlash storage, and can then be reviewed to determine the cause of network problems, identify security threats, and to maintain efficient data transmission over the network. For more information about the configuration and use of packet capturing, refer to *Packet Capture Command Set on page 4450* or the configuration guide *Configuring Packet Capture in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the standard packet-capture **7CAPTURE** and enters the packet-capture configuration mode:

(config)#**packet-capture 7CAPTURE standard**
(config-packet-capture-7CAPTURE)#

policer <*name*>

Use the **policer** command to create a Layer 2/Layer 3 Ethernet virtual connection (EVC) policer policy and enter the Layer2/Layer 3 EVC Policer Policy Configuration mode. The EVC policer policy limits the amount of traffic outbound from the AOS unit to the Metro Ethernet network (MEN). Using the **no** form of this command removes the EVC policer policy from the AOS unit's configuration. Variations of this command include:

policer <*name*>
policer <*name*> <*slot*>

Syntax Description

<*name*>	Specifies the name of the EVC policer policy.
<*slot*>	Optional. Identifies the slot on which to apply the EVC policer policy.

Default Values

By default, no EVC policer policies are configured.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

The EVC policer policy can limit traffic on EVCs, user network interfaces (UNIs), or EVC maps based on traffic committed burst size (CBS), committed information rate (CIR), excess burst size (EBS), and excess information rate (EIR). These thresholds are used to determine when the EVC bandwidth usage is too great, and the traffic is either queued or dropped based on the configured thresholds. For more information about the configuration and use of EVC policer policies, refer to *MEF Policer Policy Command Set on page 3684*.

Usage Examples

The following example creates the EVC policer policy **Policy1** and enters the Layer 2/Layer 3 EVC Policer Policy Configuration mode:

```
(config)#policer Policer1
(config-policer Policer1)#
```


policy-class max-sessions *<number>*

Use the **policy-class max-sessions** command to specify the maximum number of allowed policy sessions in the AOS product for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) combined. This command sets the maximum session limit for ALL access control policies (ACPs) on the AOS unit. To set the maximum number of policy sessions only for IPv4, use the command *ip policy-class <ipv4 acp name> max-sessions <number> on page 1437*. To set the maximum number of policy sessions only for IPv6, use the command *ipv6 policy-class <ipv6 acp name> max-sessions <number> on page 1550*. Use the **no** form of this command to return to the default value.

Syntax Description

<number>	Specifies the number of allowed ACP sessions. Valid range is **1** to a value based on the amount of RAM in the AOS unit (refer to *Default Values* below).

Default Values

By default, the maximum IPv4 and IPv6 ACP sessions allowed are based on the amount of RAM in the AOS unit. The following table outlines the default values based on RAM:

RAM Amount	Default Max Sessions
64 MB	10000
128 MB	30000
256 MB	80000
512 MB	200000
768 MB	300000
1 GB	450000

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example sets the maximum number of ACP sessions allowed in the AOS unit (for both IPv4 and IPv6 ACP sessions) to **250000**:

(config)**#policy-class max-sessions 250000**

portal-list *<name> <portal1 portal2 portal3>*

Use the **portal-list** command to create a portal list to associate with a local user name. Use the command *username <username> password <password> on page 1887* to assign this portal list to an previously configured user name. Use the **no** form of this command to remove the portal list.

> NOTE *Entering this command with the same name, but a different portal list will overwrite the original portal list.*

Syntax Description

<name>	Specifies the name of the portal list (maximum of 80 characters).
<portal>	Specifies the portals assigned to this portal list. The list can contain any combination of the portals listed below:
console	Allows the list holder to access the unit via the console.
ftp	Allows the list holder to access the unit via File Transfer Protocol (FTP).
http-admin	Allows the list holder to view the configuration and statistics via Hypertext Transfer Protocol (HTTP).
ssh	Allows the list holder to access the unit via secure shell (SSH).
telnet	Allows the list holder to access the unit via Telnet.

Default Values

By default, no portal lists are defined.

Command History

Release 17.1	Command was introduced.

Functional Notes

The same portal list can be assigned to multiple user names. Once the list is assigned to the user name, that user name can only authenticate the portals in the list. If a list is not assigned to a user name, that user name can be used with any portal that is set for local login.

Usage Examples

The following example assigns the **console**, **telnet**, and **ssh** portals the portal list **engineers**:

(config)**#portal-list engineers console telnet ssh**

port-auth default

Use the **port-auth default** command to set all global port-authentication settings to their default states.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets all global port-authentication settings to their default states:

(config)**#port-auth default**

port-auth max-req <*number*>

Use the **port-auth max-req** command to specify the maximum number of identity requests the authenticator will transmit before restarting the authentication process. Use the **no** form of this command to return to the default setting.

Syntax Description

<*number*>	Specifies the maximum number of authentication requests.

Default Values

By default, the maximum number of authentication requests is set at 2.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the maximum number of authentication requests at **4**:

(config)**#port-auth max-req 4**

port-auth re-authentication

Use the **port-auth re-authentication** command to enable re-authentication. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, re-authentication is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables re-authentication:

(config)**#port-auth re-authentication**

port-auth supplicant

Use the **port-auth supplicant** command to enable the port-authentication supplicant mode feature and to enter the Port-Authentication Supplicant Configuration mode. Use the **no** form of this command to remove the supplicant mode parameters. Variations of this command include:

port-auth supplicant
port-auth supplicant username <*username*> **password** <*password*>

Syntax Description

supplicant	Specifies that port authentication is in supplicant mode.
username <*username*>	Specifies the user name used for supplicant authentication.
password <*password*>	Specifies the password used for supplicant authentication.

Default Values

By default, port authentication and port authentication supplicant mode is disabled.

Command History

Release 10.1	Command was introduced.

Functional Notes

The supplicant user name and password can be stored in the port and set in the session if it exists. This allows for the user name and password to be set before the supplicant functionality is enabled.

Usage Examples

The following example sets the user name of **admin** and the password of **password** for supplicant mode authentication on the **eth 0/1** interface:

(config)**#interface eth 0/1**
(config-eth-0/1)**#port-auth supplicant username admin password password**

port-auth timeout

Use the **port-auth timeout** command to configure various port authentication timers. Use the **no** form of this command to return to the default setting. Variations of this command include:

port-auth timeout quiet-period <*value*>
port-auth timeout re-authperiod <*value*>
port-auth timeout tx-period <*value*>

Syntax Description

quiet-period <*value*>	Specifies the amount of time the system will wait before attempting another authentication once a failure has occurred. Range is **1** to **65535** seconds.
re-authperiod <*value*>	Specifies the amount of time between scheduled re-authentication attempts. Range is **1** to **4294967295** seconds.
tx-period <*value*>	Specifies the amount of time the authenticator will wait between identity requests. Range is **1** to **65535** seconds.

Default Values

By default, **quiet-period** is set to 60 seconds, **re-authperiod** is set to 3600 seconds (1 hour), and **tx-period** is set to 30 seconds.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the quiet-period to **10** seconds:

(config)**#port-auth timeout quiet-period 10**

port-channel load-balance

Use the **port-channel load-balance** command to configure port aggregation load distribution. Use the **no** form of this command to reset distribution to its default setting. Variations of this command include:

port-channel load-balance dst-mac
port-channel load-balance src-mac

Syntax Description

dst-mac	Specifies the destination medium access control (MAC) address.
src-mac	Specifies the source MAC address.

Default Values

By default, load balance is set to **src-mac**.

Command History

Release 5.1	Command was introduced.

Functional Notes

During port aggregation, the port channel interface must determine on which physical port to transmit packets. With the source-address configuration, the source MAC address of the received packets is used to determine this allocation. Packets coming from a specific host always use the same physical port. Likewise, when the destination address configuration is used, packets are forwarded based on the MAC address of the destination. Packets destined for a specific host always use the same physical port.

Usage Examples

The following example sets the load distribution to use the destination MAC address:

(config)**#port-channel load-balance dst-mac**

power-supply shutdown automatic

Use the **power-supply shutdown automatic** command to enable the power supplies to automatically shut down when the unit temperature exceeds the maximum operating temperature. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables the power supplies to shut down automatically if the temperature gets too high:

(config)**#power-supply shutdown automatic**

privilege <*mode*> level <*level*>

Use the **privilege level** command to assigned a privilege level to specific commands. The exact command mode name is required to identify the correct commands or command string. The command mode can be learned using the command *show command-mode on page 584*. Variations of this command include:

privilege <*mode*> **all level** <*level*>
privilege <*mode*> **all level** <*level*> <*command string*>
privilege <*mode*> **level** <*level*> <*command string*>

The following command strings cannot have their privilege levels changed: ***exit****,* ***enable****,* ***logout****, and* ***do****.*

Syntax Description

<*mode*>	Specifies the exact command mode name to which the command or command string belongs. Refer to the *Functional Notes* below for more information.
all	Specifies the privilege level be applied to all commands in the specified command mode. When used in conjunction with the <*command string*> variable, the privilege level is applied to only the parameters beyond the specified command string. Refer to the examples in the *Functional Notes* and *Usage Examples* below for more details.
level <*level*>	Specifies the privilege level to be applied to the commands. Valid range is **1** through **7**.
<*command string*>	Optional. Specifies the command string to which the privilege level is to be applied. This can include the full command string or partial command string. Refer to the examples in the *Functional Notes* and *Usage Examples* below for more details.

Default Values

By default, privilege levels are set to **1** for commands in the **exec** command mode and **7** for all other command modes.

Command History

Release R10.11.0	Command was introduced.
Release R11.3.0	Command was altered. The <*command string*> variable is no longer required, but is optional. This allows the **all** keyword to be used to specify changing the privilege level for all commands in a command mode.
Release R11.5.0	Command was expanded to include the Secure Realtime Transfer Protocol (SRTP) and Transport Layer Security (TLS) profile command modes as well as the standard Media Access Control (MAC) hardware access control list (ACL) command set.
Release R11.7.0	Command was expanded to include the 10 gigabit switchport interface.

Release R11.9.0	Command was expanded to include the **crypto-ipsec-profile**, **tunnel-gre** and **tunnel-mgre** command sets.
Release R11.10.0	Command was expanded to include the battery command set.
Release R11.11.0	Command was expanded to include the tunnel interface.

Functional Notes

The command mode name must be entered exactly in order to execute this command. Because the available command modes differ between AOS products, the most reliable method for learning the available command mode names is to use the CLI help. Enter the **privilege ?** command to display a list of all available command modes on the AOS device. Refer to the *Configuring Privilege Levels in AOS* configuration guide for more information.

The **all** keyword is useful for changing the privilege level on all commands within a command mode. For example, to assign all commands in the **interface-gigabit-ethernet** command mode to privilege level 3, enter the following command:

(config)**#privilege interface-gigabit-ethernet all level 3**

When used in conjunction with the <*command string*> variable, the **all** keyword changes the privilege level for a group of commands with several parameters, such as **show** or **debug** commands. For example, to assign all **show** commands a privilege level **5**, enter the following command:

(config)**#privilege exec all level 5 show**

The command string can include more specific parameters to reduce the number of commands affected. For example, entering **privilege exec all level 5 show ip route**, assigns the following list of commands a privilege level **5**:

show ip route
show ip route <*ipv4 address*>
show ip route <*ipv4 address*> <*subnet mask*>
show ip route <*ipv4 address*> **longer-prefixes**
show ip route <*ipv4 address*> <*subnet mask*> **longer-prefixes**
show ip route bgp
show ip route bgp verbose
show ip route connected
show ip route ospf
show ip route ospf verbose
show ip route rip
show ip route rip verbose
show ip route static
show ip route static verbose
show ip route summary
show ip route summary realtime
show ip route table
show ip route vrf <*name*>
show ip route vrf <*name*> <*ipv4 address*>
show ip route vrf <*name*> <*ipv4 address*> <*subnet mask*>

show ip route vrf <*name*> <*ipv4 address*> **longer-prefixes**
show ip route vrf <*name*> <*ipv4 address*> <*subnet mask*> **longer-prefixes**
show ip route vrf <*name*> **bgp**
show ip route vrf <*name*> **connected**
show ip route vrf <*name*> **ospf**
show ip route vrf <*name*> **rip**
show ip route vrf <*name*> **static**
show ip route vrf <*name*> **summary**
show ip route vrf <*name*> **table**

Any future AOS firmware updates in which new commands are introduced, will require the new commands to be altered as necessary related to this privilege level configuration.

Usage Examples

The following example assigns the privilege level **3** to all commands within the Ethernet Interface Configuration mode:

(config)**#privilege interface-ethernet all level 3**

The following example assigns the privilege level **3** to the **shutdown** command from within the Ethernet Interface Configuration mode:

(config)**#privilege interface-ethernet level 3 shutdown**

The following example assigns the privilege level **3** to all **show ip route** command parameters by using the **all** keyword:

(config)**#privilege exec all level 3 show ip route**

probe

Use the **probe** command to create a probe as part of network monitoring. This command is also used to enter into the Network Monitoring Probe command set once a probe is created. A probe can be one of five types: **http-request**, **icmp-echo**, **icmp-timestamp**, **tcp-connect**, or **twamp**. Each probe type has a set of commands used for configuration. These additional commands are covered in *Network Monitor Probe Command Set on page 4062*. Use the **no** form of this command to delete the probe. Variations of this command include:

probe <*name*> **http-request**
probe <*name*> **icmp-echo**
probe <*name*> **icmp-timestamp**
probe <*name*> **tcp-connect**
probe <*name*> **twamp**

*Issue the **no shutdown** command to activate the probe once it is configured. Issuing the **shutdown** command at the probe configuration prompt will disable a probe, causing it to cease generating traffic. While a probe is shut down, it will return a fail value to a track.*

The probe is not operational until tolerance is defined. Refer to Network Monitor Probe Command Set on page 4062 for more information.

Syntax Description

<name>	Specifies the name of the probe being created, or indicates the probe affected by the commands that follow.
http-request	Specifies the probe type being created as an Hypertext Transfer Protocol (HTTP) request.
icmp-echo	Specifies the probe type being created as an Internet Control Message Protocol (ICMP) echo.
icmp-timestamp	Specifies the probe type being created as an ICMP timestamp.
tcp-connect	Specifies the probe type being created as a Transmission Control Protocol (TCP) connect.
twamp	Specifies the probe type being created as a Two-Way Active Measurement Protocol (TWAMP).

Default Values

By default, there are no probes configured.

Command History

Release 13.1	Command was introduced.
Release 17.2	Command was expanded to include the ICMP timestamp and TWAMP probe types.

Usage Examples

The following example creates an ICMP echo probe called **probe1**:

>**enable**
#configure terminal
(config)**#probe probe1 icmp-echo**
(config-probe-probe1)#

Technology Review

Probes are standalone objects that help determine the status of a route based on the success or failure of probe traffic across the path. The probes can be configured to trigger at particular intervals. There are three types of probes supported by AOS: **icmp-echo**, **tcp-connect**, and **http-request**. Commands common to all the probe types are identified in the following section, as well as isolated commands that only apply to the specific probe types.

Additional configuration commands are available for associating tracks with each probe. These are explained in the *Network Monitor Track Command Set on page 4098*.

probe responder

Use the **probe responder** command to enable a probe responder to respond to specific probe packets. Additional commands for each responder type are covered in *Network Monitor Probe Responder Command Set on page 4089*. Use the **no** form of this command to stop the probe responder from responding to the specific probe packets. Variations of this command include:

probe responder icmp-timestamp
probe responder twamp
probe responder udp-echo

*Issue the **no shutdown** command to activate the probe responder once it is configured. By default, probe responders are shut down when created. Issuing the **shutdown** command disables the probe responder and it will not respond to packets.*

Syntax Description

icmp-timestamp	Specifies the probe responder type as Internet Control Message Protocol (ICMP) timestamp.
twamp	Specifies the probe responder type as Two-Way Active Measurement Protocol (TWAMP).
udp-echo	Specifies the probe responder type as a User Datagram Protocol (UDP) echo.

Default Values

By default, there are no probe responders enabled.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example enables the UDP echo probe responder:

>**enable**
#configure terminal
(config)**#probe responder udp-echo**
(config-probe-probe1)#

procare

Use the **procare** command to sync a device with an activated, qualifying ProCare plan with Adtran's ProCare server and enable the configuration backup service. For more information about verifying and activating your ProCare plan, refer to the *Functional Notes* below. The backup service retains the last saved configuration of the AOS device on the Adtran ProCare hosted infrastructure.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

Only devices covered by an activated, qualifying ProCare plan will be able to communicate with the ProCare hosted infrastructure. For more information about ProCare plans, visit www.adtran.com/procare. Configuration backup service is not offered with ProCare Basic plans. To confirm or request activation, email ProCareBackups@adtran.com and include your name, phone number, unit serial number, and the public IP address for the device. To purchase a ProCare plan, please contact your preferred partner. For a list of partners, click on the Where to Buy link at www.adtran.com.

To connect to Adtran ProCare, your device must have an Internet connection with a public IP address that is not 0.0.0.0.

Usage Examples

The following example enables the configuration backup service:

<config>**#procare**

procloud

Use the **procloud** command to connect an AOS device to Adtran ProCloud service. For more information about verifying and activating ProCloud, refer to the *Functional Notes* below.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

Adtran's ProCloud service offers hosted, managed cloud network services. Only devices with qualifying ProCloud coverage can use this service. To validate your coverage, call 1-800-874-2237, email serviceplan@adtran.com, or visit the Service Plan Portal at www.adtran.com/serviceplan. To purchase a ProCloud plan, please contact your preferred partner. For a list of partners, click on the Where to Buy link at www.adtran.com.

To connect to Adtran ProCloud LAN, your device must have an Internet connection with a public IP address that is not 0.0.0.0.

Usage Examples

The following example connects the device to the Adtran ProCloud service:

<config>**#procloud**

qos cos-map *<cos queue id> <cos value>*

Use the **qos cos-map** command to associate class of service (CoS) values with each queue. Use the **no** form of this command to return to the default setting.

Syntax Description

<cos queue id>	Specifies the queue number that you are assigning CoS value(s).
<cos value>	Associates listed CoS values with a particular priority queue. Multiple CoS values can be applied to a specified queue. Valid range is **0** to **7**.

Default Values

On NetVanta switch products, there are four queues and the default CoS value mapped to each queue are as outlined below:

Queue 1 is mapped to CoS 0 and 1

Queue 2 is mapped to CoS 2 and 3

Queue 3 is mapped to CoS 4 and 5

Queue 4 is mapped to CoS 6 and 7

On carrier Ethernet products, there are eight queues and the default CoS values mapped to each queue are as outlined below:

Queue 0 is mapped to CoS 1

Queue 1 is mapped to CoS 0

Queue 2 is mapped to CoS 2

Queue 3 is mapped to CoS 3

Queue 4 is mapped to CoS 4

Queue 5 is mapped to CoS 5

Queue 6 is mapped to CoS 6

Queue 7 is mapped to CoS 7

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example maps CoS values 4 and 5 to queue 1:

(config)#**qos cos-map 1 4 5**

qos dscp-cos

Use the **qos dscp-cos** command to set the differentiated services code point (DSCP) to class of service (CoS) map and enable the mapping process. Use the **no** form of this command to disable mapping. Variations of this command include:

qos dscp-cos <*dscp value*> **to** <*cos value*>
qos dscp-cos default

Syntax Description

<*dscp value*>	Specifies DSCP values (separating multiple values with a space). Valid range is **0** to **63**.
<*cos value*>	Specifies CoS values (separating multiple values with a space). Valid range is **0** to **7**.
default	Sets the map to the following default values: DSCP 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 CoS 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

When one of the specified DSCP values is detected in an incoming packet, the CoS priority is altered based on the corresponding map value. By configuring the list, the mapping functionality is enabled.

Usage Examples

The following example enables the mapping of DSCP values 24 and 48 to CoS values 1 and 2:

(config)**#qos dscp-cos 24 48 to 1 2**

The following example disables DSCP-to-CoS mapping:

(config)**#no qos dscp-cos**

qos map <*name*> <*number*>

Use the **qos map** command to create a quality of service (QoS) map and activate the QoS Map Command Set (which allows you to edit a QoS map). For details on specific commands, refer to the *Quality of Service Map Command Set on page 4464*. Use the **no** form of this command to delete a map entry. Variations of this command include:

qos map <*name*> <*number*>
qos map <*name*> <*number*> **match-all**
qos map <*name*> <*number*> **match-any**

Syntax Description

<*name*>	Specifies the QoS map name.
<*number*>	Assigns a sequence number to differentiate this QoS map and provide a match order. Valid range is **0** to **65535**.
match-all	Optional. Indicates the traffic must match all conditions before the set action is issued.
match-any	Optional. Indicates the traffic can match any of the conditions to be processed, which is the default behavior.

Default Values

By default, there are no QoS maps defined. Once created, the default behavior is to match any of the conditions set for the QoS map.

Command History

Release 6.1	Command was introduced.
Release 17.2	Command was expanded to include the **match-all** and **match-any** parameters.

Functional Notes

AOS uses QoS maps to classify packets into groups for matching. A QoS map contains multiple class entries, each of which has packet match cases, and a set of actions for the particular group (actions are defined by **bandwidth**, **priority**, **set**, and **shape** commands). Multiple map entries for the same QoS map are differentiated by a sequence number. The sequence number is used to assign the order in which the conditions are matched.

Once created, a QoS map must be applied to an interface (using the **qos-policy out** command) in order to actively process traffic. Refer to *qos-policy on page 2306* for more information on assigning the map to an interface. Any traffic for the interface that is not sent to the priority queue is sent using the default queuing method for the interface (such as weighted fair queuing (WFQ)).

Usage Examples

The following example demonstrates basic settings for a QoS map and assigns a map to the Frame Relay interface:

>**enable**
#config terminal
(config)**#qos map VOICEMAP 10**
(config-qos-map)**#match precedence 5**
(config-qos-map)**#priority 512**
(config-qos-map)**#exit**
(config)**#interface fr 1**
(config-fr 1)**#qos-policy out VOICEMAP**

qos policer mode non-bias

Use the **qos policer mode non-bias** command to specify the policer algorithm used in Metro Ethernet Forum (MEF) policer quality of service (QoS) configurations. Use the **no** form of this command to specify the policer uses the MEF10 reference algorithm.

Syntax Description

No subcommands.

Default Values

By default, the MEF policer is configured to use the **non-bias** setting.

Command History

Release R11.5.2	Command was introduced.

Functional Notes

This command configures the AOS device to use a policer algorithm that largely eliminates the MEF10 policer algorithm's bias for small frames. When a policer drops a packet in a flow, it drops all subsequent packets in the flow until the policer credit builds up to at least the hardware maximum transmission unit (MTU). Prior to AOS release R11.6.0, the hardware MTU was set to 2000 bytes. After AOS release R11.6.0, the hardware MTU is set to 9200 bytes to allow for jumbo frames. When the **no** form of this command is used, the policer uses the MEF10 reference algorithm, which has a bias for small frames over large frames.

Usage Examples

The following example specifies that the MEF policer uses the MEF10 reference algorithm:

(config)**#no qos policer mode non-bias**

qos queue-type strict-priority

Use the **qos queue-type strict-priority** command to enable queuing based strictly on the priority of each queue. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the queue type is weighted round robin (WRR).

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables strict-priority queuing:

(config)**#qos queue-type strict-priority**

qos queue-type wrr

Use the **qos queue-type wrr** command to set weights for up to four queues. Use the **no** form of this command to set all queues to be weighted round robin (WRR). Variations of this command include:

qos queue-type wrr <*weight1*> <*weight2*> <*weight3*> **expedite**
qos queue-type wrr <*weight1*> <*weight2*> <*weight3*> <*weight4*>

Syntax Description

<*weight1-4*>	Sets the weight of each queue (up to four). All queue weights must be greater than zero, except for the weight for the last queue (queue 4). The range for queues 1 to 3 is 1 to 255. The range for queue 4 is **0** to **255**.
expedite	The queue 4 entry can be replaced by the **expedite** command. If set to **expedite**, then it becomes a high-priority queue. All outbound traffic is transmitted on an expedite queue prior to any other traffic in other queues.

Default Values

By default, all four weights are set to **25**.

Command History

Release 5.1	Command was introduced.

Functional Notes

The actual weight is a calculated value based on the sum of all entered weights. It is the ratio of the individual weight over the sum of all weights.

For example:

If the user enters 10, 20, 30, and 40 as the weight values, the first queue will have a ratio of 1/10. This is derived from the formula 10/(10+20+30+40). Therefore, this queue will transmit 1 packet out of every 10 opportunities.

Usage Examples

The following example configures weights for all four queues:

(config)**#qos queue-type wrr 10 20 30 40**

queue interface

Use the **queue interface** command to configure a queue on an interface. Use the **no** form of this command to remove the queue configuration on the interface. Variations of this command include:

queue interface efm-group <*slot/group*> <*queue*>
queue interface gigabit-ethernet <*slot/port*> <*queue*>

Syntax Description

efm-group <*slot/group*>	Specifies the queue is configured on an Ethernet in the first mile (EFM) group interface. Group range is **1** to **1024**.
gigabit-ethernet <*slot/port*>	Specifies the Gigabit Ethernet interface on which to configure the queue.
<*queue*>	Specifies the queue to configure. Carrier Ethernet products have eight queues, with a valid range of **0** to **7**.

Default Values

By default, no queues on configured on the EFM group or Gigabit Ethernet interfaces.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

Once you have entered the **queue interface** command, you can configure the queue from the Ethernet virtual connection (EVC) Queue Configuration mode. Refer to *Carrier Ethernet Queue Command Set on page 3728* for queue configuration commands.

Usage Examples

The following example enters the queue's configuration mode on an EFM group interface:

```
(config)#queue interface efm-group 1/1 5
(config-queue 5)#
```


queue time-constant wred <*value*>

Use the **queue time-constant wred** command to configure the weighted random early detection (WRED) time constant used to calculate the average queue depth for all queues.

Syntax Description

<*value*>	Specifies the time constant used to calculate the average queue depth for all queues. Accepted values are **2**, **4**, **8**, **16**, **32**, **62**, **125**, **250**, and **500** milliseconds (ms).

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

The WRED time constant allows the user to adjust the time component used to calculate the average queue depth. For example, if the WRED time constant is set to **8** ms, the queue depth will be the average number of packets over an 8 ms period of time. If the WRED time constant is set too low, bursty traffic may inadvertently be marked for discard. Conversely, if the WRED time constant is set too high, traffic may remain in the queue substantially longer than usual which can impact Transmission Control Protocol (TCP) throughput. Adtran recommends setting the WRED time constant to the approximate round trip delay for TCP packets.

Usage Examples

The following example sets the WRED queue time constant to **62** ms.

(config)**#queue time-constant wred 62**

radius-server

Use the **radius-server** command to configure several remote authentication dial-in user service (RADIUS) parameters for all RADIUS servers on the network. Most of these global settings can be overridden on a per-server basis (using the command *radius-server host on page 1682*). Use the **no** form of this command to return to the default setting. Variations of this command include the following:

radius-server challenge-noecho
radius-server deadtime <*value*>
radius-server enable-username <*name*>
radius-server key <*key*>
radius-server retry <*number*>
radius-server timeout <*value*>

Syntax Description

challenge-noecho	Specifies that when users enter text in response to challenge questions the entered text does not appear on the screen.
deadtime <*value*>	Specifies the time to wait (in minutes) before attempting to reconnect to a RADIUS server that has timed out. Range is **0** to **1440** minutes. Changing this parameter changes the time to wait for all configured RADIUS servers.
enable-username <*name*>	Specifies a user name to be used for authentication to enter the Enable mode. This user name is the name sent for AAA Enable mode access requests. Changing this parameter changes the user name for all configured RADIUS servers.
key <*key*>	Specifies the encryption key shared by all RADIUS servers. This is a global setting; however, it can be overridden on a per-server basis.
retry <*number*>	Specifies the number of connection attempts to a RADIUS server. Attempt range is **0** to **10**. This is a global setting; however, it can be overridden on a per-server basis.
timeout <*value*>	Specifies the amount of time (in seconds) that RADIUS servers have to respond to a request. Time range is **1** to **1000** seconds. This is a global setting; however, it can be overridden on a per-server basis.

Default Values

challenge-noecho	Echo is disabled and users do not see on-screen what they enter.
deadtime	**0** minutes
enable-username	**$enab15$**
key	No default
retry	**0** attempts
timeout	**5** seconds

Command History

Release 5.1	Command was introduced.
Release 7.1	Added the **enable-username** selection.

Functional Notes

It is recommended that you use a user name that is a unique name for your network and one that only the network administrators know. If the default user name is used, it is possible for unauthorized users to gain access to the network.

By default, there is a **0** minute wait time before attempting to reconnect to a timed out server. Leaving the wait time at **0** minutes means that the server will never be declared dead. The time period value is **0** to **1440** minutes, although you should enter a value of at least **1** minute or greater.

Usage Examples

The following example shows a typical configuration of these parameters:

(config)**#radius-server deadtime 10**
(config)**#radius-server enable-username fantastico**
(config)**#radius-server key mysecretkey**
(config)**#radius-server retry 4**
(config)**#radius-server timeout 2**

radius-server host

Use the **radius-server host** command to specify the parameters for a remote authentication dial-in user service (RADIUS) server. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the configuration to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the settings to the default unnamed VRF. Use the **no** form of this command to return to the default setting. Variations of this command include:

radius-server host <*hostname* | *ip address*>
radius-server host <*hostname* | *ip address*> **acct-port** <*port*>
radius-server host <*hostname* | *ip address*> **auth-port** <*port*>
radius-server host <*hostname* | *ip address*> **key** <*key*>
radius-server host <*hostname* | *ip address*> **retransmit** <*number*>
radius-server host <*hostname* | *ip address*> **timeout** <*value*>
radius-server vrf <*name*> **host** <*hostname* | *ip address*>
radius-server vrf <*name*> **host** <*hostname* | *ip address*> **acct-port** <*port*>
radius-server vrf <*name*> **host** <*hostname* | *ip address*> **auth-port** <*port*>
radius-server vrf <*name*> **host** <*hostname* | *ip address*> **key** <*key*>
radius-server vrf <*name*> **host** <*hostname* | *ip address*> **retransmit** <*number*>
radius-server vrf <*name*> **host** <*hostname* | *ip address*> **timeout** <*value*>

Each parameter after <hostname | ip address> specifies the characteristics of the individual RADIUS server. Parameters can be entered in a single command line, in any order, but each may only be used once.

Syntax Description

<*hostname* | *ip address*>	Specifies the server to configure. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the AOS device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the command *name-server on page 1622*.
acct-port <*port*>	Specifies the User Datagram Protocol (UDP) port used by the AAA accounting server. Port range is **0** to **65535**. This command is reserved for future use as currently AOS does not allow RADIUS servers for use with AAA accounting.
auth-port <*port*>	Specifies the UDP port used by the AAA authentication server. The port range is **0** to **65535**.
key <*key*>	Specifies the encryption key used by the RADIUS server. This command overrides the global RADIUS key setting (set with the command *radius-server on page 1680*). This command must be entered last in the command line because everything after the **key** parameter is read as the new key.
retransmit <*number*>	Specifies the number of connection attempts made to the server. Attempt range is **1** to **100**.

timeout <*value*>	Specifies the time to wait (in seconds) for this server to reply to requests. Range is **1** to **1000** seconds.
vrf <*name*>	Specifies the name of the VRF to which to assign the association. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, **acct-port** is set to **1813** and **auth-port** is set to **1812**. By default, the key, retransmit and timeout values are the values set by the command *radius-server on page 1680*.

Command History

Release 5.1	Command was introduced.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

At a minimum, the address (IP or host name) of the server must be given. The other parameters can be entered in any order (except the **key** parameter) and, if the parameters are not specified, they will take default values or fall back on the global RADIUS server's default settings (set using the command *radius-server on page 1680*).

If global password protection is enabled on the AOS device, encryption will be applied to the authentication key (**key** <*key*>). If global password protection is off, the authentication key will display as clear text. Refer to *service password-encryption on page 1699* for more information

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example specifies that the RADIUS server at IP address **10.10.10.2** uses the global key setting (left unspecified), a timeout value of **10** seconds, the default authorization port (left unspecified), and a retransmit number of **5**:

(config)**#radius-server host 10.10.10.2 retransmit 5 timeout 10**

The following example specifies that the RADIUS server at IP address **10.10.10.2** on VRF **RED**, uses the global key setting (left unspecified), a timeout value of **10** seconds, the default authorization port (left unspecified), and a retransmit number of **5**:

(config)**#radius-server vrf RED host 10.10.10.2 retransmit 5 timeout 10**

resource-utilization

Use the **resource-utilization** command to set a threshold limit for CPU or heap utilization notifications. When the utilization threshold is surpassed, a resource trap is sent. Use the **no** form of this command to remove the threshold setting. Variations of this command include:

resource-utilization cpu threshold <*percentage*> **time-interval** <*value*>
resource-utilization heap threshold <*percentage*>

Syntax Description

cpu	Sets the threshold for CPU utilization notification.
heap	Sets the threshold for heap utilization notification.
threshold <*percentage*>	Specifies the threshold limit as a percentage of resource utilization. Valid range is **1** to **100** percent.
time-interval <*value*>	Specifies the time interval for the actual utilization to exceed the threshold before a notification is sent. Valid range is **1** to **86400** seconds.

Default Values

By default, there are no thresholds configured.

Command History

Release A2.04	Command was introduced.

Functional Notes

Simple Network Management Protocol (SNMP) resource traps must be enabled before exceeded threshold notifications are sent. Refer to *snmp-server enable traps on page 1792*.

Usage Examples

The following example configures the CPU resource notification to be sent when the CPU usage maintains at least 75 percent utilization for 40 seconds:

(config)**#resource-utilization cpu threshold 75 time-interval 40**

restricted boot

Use the **restricted boot** command to restrict issuing specific bootcode commands. Refer to the *Functional Notes* below. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release R11.4.0	Command was introduced.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

Once enabled, the restricted boot feature will prohibit a user from performing any of the following functions in bootcode:

- Bypass password option
- Bypass startup-config option
- Erase or overwrite individual files
- Copy files from flash

*The **erase file-system** and **erase *** commands are both allowed for unit recovery even when **restricted boot** is enabled.*

This command is not available in vAOS instances.

Usage Examples

The following example enables the restricted boot feature:
(config)**#restricted boot**

rtcp

Use the **rtcp** command to enable sending Realtime Transport Control Protocol (RTCP) sender reports to improve interoperation with other network equipment. The RTCP Sender Report is sent at periodic intervals when when RTP is being received. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, RTCP sender reports are disabled.

Command History

Release R11.7.0	Command was introduced.

Functional Notes

RTCP sender reports are sent for the following call scenarios:

- Session Initiation Protocol (SIP) to foreign exchange station (FXS)
- SIP to foreign exchange office (FXO)
- SIP to T1 (primary rate interface (PRI) and robbed-bit signaling (RBS))

For SIP to SIP calls, RTCP sender reports are passed through the unit unmodified.

For all supported products, the RTCP port number is the next odd port number following the even Realtime Transport Protocol (RTP) port number.

If, during a call, RTP is not being sent (i.e., RTP is receive-only), then a sender report is sent instead of a receiver report as described in RFC 3550.

Usage Examples

The following example enables the sending of RTCP sender reports:

```
(config)#rtcp
```

route-map

Use the **route-map** command to create a route map and enter the Route Map Configuration command set. A route map is a type of filter that matches various attributes and then performs actions on the way the route is redistributed. Use the **no** form of this command to delete a route map. Variations of this command include:

route-map <*name*> <*number*>
route-map <*name*> **deny** <*number*>
route-map <*name*> **permit** <*number*>

Syntax Description

<*name*>	Specifies a name for the route map.
deny	Specifies not to redistribute routes matching the route map attributes.
permit	Redistributes routes matching the route map attributes.
<*number*>	Specifies a sequence number of this route entry. Range is **1** to **4294967295**.

Default Values

By default, no route maps are defined.

Command History

Release 9.3	Command was introduced.

Functional Notes

Route maps can be used to filter inbound and outbound routes and to apply attributes to the routes being filtered. A route map applied to outbound data determines how the router advertises routes to a neighbor. The **outbound** route map can be configured to perform such tasks as:

- Define the routes that the router can advertise according to specified attributes or prefixes.
- Prepend private AS numbers to specific routes to help balance inbound traffic.
- Set an MED on specific routes to help balance inbound traffic.
- Request that the neighbor advertise the route to certain communities only.
- When a route map is applied to inbound data, it determines which of the service provider advertised routes the local router accepts.

The **inbound** route map can be configured to perform such tasks as:

- Filter external routes according to specified attributes or prefixes
- Apply attributes to filtered routes, including:
  - Local preference
  - Community
  - MED value
  - Prepended AS path
- Delete communities defined for the routes

The route map itself is created first. Matching criteria and attributes are defined within the route map configuration menu. Once a route map has been established, it can be assigned to a BGP neighbor.

Match and set commands used for filtering and defining attributes are found in the *Route Map Command Set on page 4168*.

Usage Examples

The following example creates the route map, specifies that routes matching its criteria will be denied, and assigns a sequence number of 100:

(config)**#route-map MyMap deny 100**
(config-route-map)#

You can then define the attributes of the route map from the Route Map Configuration command set. Enter a **?** at the **(config-route-map)#** prompt to explore the available options.

router bgp *<value>*

Use the **router bgp** command to enable BGP and enter the BGP Configuration mode. Refer to the *BGP Command Set on page 3981* for more information. Use the **no** form of this command to disable Border Gateway Border (BGP) routing.

Syntax Description

<value>	Specifies the AS number of the local system of which this BGP router is a member. Range is **1** to **4294967295**.

Default Values

By default, BGP is disabled.

Command History

Release 10.1	Command was introduced.
Release 18.1	Command was altered to support 4-byte AS numbers (previously AOS only supported 2-byte numbers).

Functional Notes

The AS number of the local system of which this BGP router is a member must always be entered with this command, even when re-entering BGP Configuration mode after BGP has already been activated on the router.

Usage Examples

The following example uses the **router bgp** command to enable BGP and enter the BGP Configuration mode:

```
(config)#router bgp 100
(config-bgp)#
```

router ospf *<process id>*

Use the **router ospf** command to activate Open Shortest Path First version 2 (OSPFv2) in the router and to enter the OSPF Configuration mode. This command creates a new OSPFv2 process, or allows you to edit a previously configured OSPFv2 process. Refer to the *Router OSPFv2 Command Set on page 4120* for more information. Use the **no** form of this command to remove the OSPFv3 process and all of its settings at both the global and interface level. Variations of this command include:

router ospf
router ospf *<process id>*
router ospf *<process id>* **vrf** *<name>*

Syntax Description

<process id>	Specifies a process ID for the OSPFv2 process. These IDs must be unique among all other OSPFv2 processes on the device. Valid ID range is **1** to **65535**.
vrf *<name>*	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to create the OSPFv2 process. If no VRF is specified, the process is created on the default (unnamed) VRF.

Default Values

By default, OSPF is disabled.

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the *<process id>* and **vrf** *<name>* parameters.

Functional Notes

AOS can be configured to use OSPF with the firewall enabled (using the **ip firewall** command). To do this, configure the OSPF networks as usual, specifying which networks the system will listen for and broadcast OSPF packets to. Refer to *ip firewall on page 1367* for more information.

To apply stateful inspection to packets coming into the system, create a policy class that describes the type of action desired and then associate that policy class to the particular interface (refer to *ip policy-class <ipv4 acp name> on page 1434*). The firewall is intelligent and will only allow OSPF packets that were received on an OSPF configured interface. No modification to the policy class is required to allow OSPF packets into the system.

Usage Examples

The following example uses the **router ospf** command to enter the OSPF Configuration mode:

(config)#**router ospf 1**

router ospfv3 <*process id*>

Use the **router ospfv3** command to enable Open Shortest Path First version 3 (OSPFv3), create an OSPFv3 process, and enter the router's OSPFv3 Configuration mode. This command creates a new OSPFv3 process, or allows you to edit a previously configured OSPFv3 process. Use the **no** form of this command to remove the OSPFv3 process and all of its settings at both the global and interface level. Variations of this command include:

router ospfv3 <*process id*>
router ospfv3 <*process id*> **vrf** <*name*>

Syntax Description

<*process id*>	Specifies a process ID for the OSPFv3 process. These IDs must be unique among all other OSPFv3 processes on the device. Valid ID range is **1** to **65535**.
vrf <*name*>	Optional. Specifies a nondefault virtual routing and forwarding (VRF) instance on which to create the OSPFv3 process. If no VRF is specified, the process is created on the default (unnamed) VRF.

Default Values

By default, no OSPFv3 processes or process IDs exist.

Command History

Release R10.5.0	Command was introduced.
Release R10.8.0	Command was expanded to include the **vrf** parameter.

Functional Notes

For more information about commands available in the OSPFv3 Configuration mode, refer to *Router OSPFv3 Command Set on page 4141*.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring OSPFv3 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables OSPFv3, creates the OSPFv3 process **5**, and enters the OSPFv3 Configuration mode:

```
(config)#router ospfv3 5
(config-ospfv3)#
```


router pim-sparse

Use the **router pim-sparse** command to globally enable protocol-independent multicast (PIM) on the unit and to enter the PIM Sparse Configuration mode. Use the **no** form of this command to disable PIM Sparse routing. Refer to the *Router PIM Sparse Command Set on page 4201* for more information on the subcommands for PIM Sparse Configuration mode.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Functional Notes

Additional commands for PIM are found in the related interface configuration modes. Refer to the **ip pim-sparse** commands in sections such as *Ethernet Interface Command Set on page 2156*, *Frame Relay Subinterface Command Set on page 2748*, *HDLC Interface Command Set on page 2888*, *Loopback Interface Command Set on page 2968*, *PPP Interface Command Set on page 3060*, *Tunnel Interface Command Set on page 3211*, and *VLAN Interface Command Set on page 3370* for more information.

Usage Examples

The following example uses the **router pim-sparse** command to enter the PIM Sparse Configuration mode:

```
(config)#router pim-sparse
(config-pim-sparse)#
```

router rip

Use the **router rip** command to enter the RIP Configuration mode. Use the **no** form of this command to disable Routing Information Protocol (RIP) routing. Refer to the *Router RIP Command Set on page 4205* for more information.

Syntax Description

No subcommands.

Default Values

By default, RIP is disabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example uses the **router rip** command to enter the RIP Configuration mode:

```
(config)#router rip
(config-rip)#
```

Technology Review

The RIP protocol is based on the Bellham-Ford (distance-vector) algorithm. This algorithm provides that a network will converge to the correct set of shortest routes in a finite amount of time, provided that:

Gateways continuously update their estimates of routes.

Updates are not overly delayed and are made on a regular basis.

The radius of the network is not excessive.

No further topology changes take place.

RIP is described in RFC 1058 (Version 1) and updated in RFCs 1721, 1722, and 1723 for Version 2. Version 2 includes components that ease compatibility in networks operating with RIP V1.

All advertisements occur on regular intervals (every 30 seconds). Normally, a route that is not updated for 180 seconds is considered dead. If no other update occurs in the next 60 seconds for a new and better route, the route is flushed after 240 seconds. Consider a connected route (one on a local interface). If the interface fails, an update is immediately triggered for that route only (advertised with a metric of 16).

Now consider a route that was learned and does not receive an update for 180 seconds. The route is marked for deletion, and even if it was learned on an interface, a poisoned (metric equals 16) route should be sent by itself immediately and during the next two update cycles with the remaining normal split horizon update routes. Following actual deletion, the poison reverse update ceases. If an update for a learned route is not received for 180 seconds, the route is marked for deletion. At that point, a 120-second garbage collection (GC) timer is started. During the GC timer period, expiration updates are sent with the metric for the timed-out route set to 16.

If an attached interface goes down, the associated route is immediately (within the same random five-second interval) triggered. The next regular update excludes the failed interface. This is the so-called first hand knowledge rule. If a gateway has first hand knowledge of a route failure (connected interfaces) or reestablishment, the same action is taken. A triggered update occurs, advertising the route as failed (metric equals 16) or up (normal metric) followed by the normal scheduled update.

The assumption here is that if a gateway missed the triggered update, it will eventually learn from another gateway in the standard convergence process. This conserves bandwidth.

RIP-Related Definitions:

Route	A description of the path and its cost to a network.
Gateway	A device that implements all or part of RIP (a router).
Hop	A metric that provides the integer distance (number of intervening gateways) to a destination network gateway.
Advertisement	A broadcast or multicast packet to port 520 that indicates the route for a given destination network.
Update	An advertisement sent on a regular 30-second interval, including all routes exclusive of those learned on an interface.

schedule <*name*>

Use the **schedule** command to create a general-purpose schedule. Use the **no** form of this command to delete a schedule. Variations of this command include:

schedule <*name*>

Additional subcommands are available once you have entered the Schedule Configuration mode:

absolute start <*schedule*> **end** <*schedule*>
periodic <*day*> **[**<*time*> **to** <*time*>**]**
periodic <*day*> <*time*> **to** <*day*> <*time*>
periodic <*day*> **[**<*time*> **for** <*duration*>**]**
periodic <*day*> <*time*> **for** <*duration*>
periodic <*time*> **for** <*duration*> <*day*>
periodic daily <*time*> **to** <*time*>
periodic daily <*time*> **for** <*duration*>
periodic weekday <*time*> **to** <*time*>
periodic weekday <*time*> **for** <*duration*>
periodic weekend <*time*> **to** <*time*>
periodic weekend <*time*> **for** <*duration*>
relative start-after <*delay*>

Syntax Description

<*name*>	Specifies the name of the schedule.
absolute start end	Indicates the schedule's **start** and **end** time and date values.
<*schedule*>	Specifies the start and end schedules. Schedules are expressed in the format <*time*> <*day*> <*month*> <*year*> (for example, **08:15 2 February 2007**).
<*time*>	Time is expressed in the 24-hour format hours:minutes (HH:MM) (for example, **08:15**).
<*day*>	The day of the month is expressed with a number. Range is 1 to 31.
<*month*>	The name of the month can be spelled out or abbreviated.
<*year*>	The year is expressed in the format YYYY (for example, **2007**).
periodic	Specifies the weekly behavior of the schedule by configuring start/end days, times, and duration.
to	Specifies the schedule's start/end day and time.
for <*duration*>	Specifies the schedule's duration. Duration is expressed in the 24-hour format hours:minutes (HH:MM).
daily	Optional. Specifies recurring period to be every day of the week.
weekday	Optional. Specifies recurring period to be Monday through Friday.
weekend	Optional. Specifies recurring period to be Saturday and Sunday.
<*time*>	Time is expressed in the 24-hour format hours:minutes (HH:MM) (for example, **08:15**).

<*day*>	The day of the week can be spelled out or abbreviated.
relative start-after <*delay*>	Specifies the time delay before the schedule becomes active. Valid range is **1** to **65535** seconds.

Default Values

By default, no schedules exist.

Functional Notes

Periodic schedules can be expressed in the format <*day*> <*time*> to <*day*> <*time*> (for example, **periodic monday 08:15 to wednesday 17:15**), or up to 7 days can be entered (for example, **periodic tuesday wednesday thursday 08:15 to 17:15**).

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was expanded.
Release 16.1	Command was expanded to include the **for** parameter.

Usage Examples

The following example creates a schedule **Closed** and enters the Schedule Configuration mode:

(config)**#schedule Closed**
(config-schedule-Closed)#

The following example sets the start time in the schedule named **Closed** to 8:15 a.m. on February 2, 2007, and sets the end time to 10:15 a.m. on April 2, 2007:

(config-schedule-Closed)**#absolute start 08:15 2 february 2007 end 10:15 2 april 2007**

The following example sets the recurring start and end day and time in the schedule named **Closed** to Saturday from 8:15 a.m. to 5:15 p.m.:

(config-schedule-Closed)**#periodic saturday 08:15 to 17:15**

The following example sets the execution delay for the schedule named **Closed** to **30** seconds:

(config-schedule-Closed)**#relative start-after 30**

The following example sets the duration for the schedule named **Closed** to **30** minutes at 1:00 p.m. every day of the week:

(config-schedule-Closed)**#periodic daily 13:00 for 00:30**

sdp grammar hold

Use the **sdp grammar hold** command to specify how to format hold messages in Session Description Protocol (SDP) announcements. Use the **no** form of this command to return to the default value. Variations of this command include the following:

sdp grammar hold rfc2543
sdp grammar hold rfc3264

Syntax Description

rfc2543	Specifies the use of RFC 2543 for formatting hold messages.
rfc3264	Specifies the use of RFC 3264 for formatting hold messages.

Default Values

By default, RFC 2543 is used for formatting hold messages.

Command History

Release 12.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example specifies to use RFC 3264 to format hold messages:

(config)**#sdp grammar hold rfc3264**

sdp grammar ptime

Use the **sdp grammar ptime** command to specify which packet times to send in Session Description Protocol (SDP) announcements. Use the **no** form of this command to return to the default value. Variations of this command include the following:

sdp grammar ptime explicit
sdp grammar ptime implicit

Syntax Description

explicit	Specifies sending all packet times.
implicit	Specifies sending only packet times of **10** and **30** ms.

Default Values

By default, implicit packet times are sent.

Command History

Release A4.01	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example specifies sending **explicit** packet times:

(config)**#sdp grammar ptime explicit**

service password-encryption

Use the **service password-encryption** command to turn on global password protection. Use the **no** form of this command to return to the default setting.

If you need to go back to a previous revision of the code (e.g., AOS Revision 10), this command must be disabled first. Once the service is disabled, all necessary passwords must be re-entered so that they are in the clear text form. If this is not done properly, you will not be able to log back in to the unit after you revert to a previous revision that does not support password encryption.

Syntax Description

No subcommands.

Default Values

By default, global password protection is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

When enabled, all currently configured passwords are encrypted. Also, any new passwords are encrypted after they are entered. Password encryption is applied to all passwords, including passwords for user name, Enable mode, Telnet/console, Point-to-Point Protocol (PPP), Border Gateway Protocol (BGP), and authentication keys. When passwords are encrypted, unauthorized persons cannot view them in configuration files since the encrypted form of the password is displayed in the running-config. While this provides some level of security, the encryption method used with password encryption is not a strong form of encryption so you should take additional network security measures.

You cannot recover a lost encrypted password. You must erase the startup-config and set a new password.

Usage Examples

The following example enables password encryption for all passwords on the unit:

(config)**#service password-encryption**

sfp trap threshold alarm time-interval <*value*>

Use the **sfp trap threshold alarm time-interval** command to set the polling interval for monitoring the sfp alarm thresholds. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the minimum polling interval in seconds. Valid range is from **1** to **86400** seconds.

Default Values

By default, the alarm polling interval is **300** seconds.

Command History

Release 13.3.0	Command was introduced.

Usage Examples

The following example configures the sfp trap threshold alarm polling interval to 600 seconds:

(config)**#sfp trap threshold alarm time-interval 600**

shaper <*name*>

Use the **shaper** command to create an Ethernet virtual connection (EVC) rate shaper and enter the shaper configuration mode. Use the **no** form of this command to remove the shaper. Variations of this command include:

shaper <*name*>
shaper <*name*> <*slot*>

Syntax Description

<*name*>	Specifies the name of the rate shaper.
<*slot*>	Optional. Specifies the slot to which the rate shaper is applied.

Default Values

By default, no EVC shapers are configured.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example creates an EVC rate shaper named **Shaper1** on slot **0**:

(config)**#shaper Shaper1 0**

Technology Review

Rate shaping is a mechanism designed to smooth out bursts of traffic. Unlike a policer, which discards large bursts of traffic, a shaper is able to delay bursts. The port shaper uses a token bucket, much like a policer, however when large bursts are received, the packets are queued rather than being discarded immediately. When a packet arrives at the shaper, if there are sufficient tokens available, the packet is transmitted without delay. If there are insufficient tokens in the bucket, the packet is delayed until there are enough tokens in the bucket to allow transmission. The benefit of a shaper is that it will not drop frames with a small burst of traffic, but it does add latency. The benefit of a policer is that it does not add latency while protecting the network, but does drop any traffic that exceeds the burst capacity. Selecting one over the other is dependent on the latency and/or loss tolerance of the data. Rate shapers are much friendlier to Transmission Control Protocol (TCP) traffic flows than policers. A small delay in latency leads to better TCP Goodput than large losses of traffic that can force TCP to revert to Slow Start. Traffic may still be discarded due to the queue congestion management strategy employed.

sip

Use the **sip** command to enable the AOS Session Initiation Protocol (SIP) stack and to specify the protocol and port used by the SIP stack. When the SIP stack is enabled, memory is allocated for SIP functionality. Use the **no** form of this command to disable the SIP stack and free the memory allocated to the stack. Variations of this command include:

sip
sip tcp
sip tcp <*port*>
sip udp
sip udp <*port*>
sip vrf <*name*>

Syntax Description

tcp	Optional. Specifies that the SIP stack operates using Transmission Control Protocol (TCP).
udp	Optional. Specifies that the SIP stack operates using User Datagram Protocol (UDP).
<*port*>	Optional. Specifies the TCP or UDP port used by the SIP stack. Range is **1** to **65535**.
vrf <*name*>	Optional. Enables the SIP stack on the specified nondefault virtual routing and forwarding (VRF) instance.

Default Values

By default, the SIP stack is enabled on AOS voice products and disabled on AOS data products. The SIP stack operates using UDP on port **5060** if no protocol or port are specified. If a protocol is specified, but no port is specified, the SIP stack uses port **5060**.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was expanded to include the **tcp**, **udp**, and <*port*> parameters.
Release R10.5.0	Command was expanded to include the **vrf** parameter.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

By default, the AOS SIP application layer gateway (ALG) is enabled. This ALG allows the firewall to examine all SIP packets it identifies and to maintain information of SIP transmissions on the network based on the SIP header. The SIP ALG requires the use of the SIP stack and the SIP proxy server in order to properly route SIP calls and maintain the SIP information. For more details on the operation of SIP and the SIP ALG, refer to the command *ip firewall alg on page 1373*.

For proper SIP operation, the firewall must also be configured to allow for dynamic holes for the Realtime Transfer Protocol (RTP) and the Realtime Transfer Control Protocol (RTCP) traffic associated with SIP calls between user agents. This functionality must be manually enabled. For more details on enabling this functionality, refer to the command *ip rtp firewall-traversal on page 1456*.

The SIP stack is used for many AOS features, including Transparent Proxy and Voice Quality Monitoring (VQM) Reporting. Refer to the configuration guides available online at https://supportcommunity.adtran.com for more information about SIP operation with specific features.

Usage Examples

The following example enables the SIP stack and specifies that the stack operates using TCP:

(config)**#sip tcp**

sip access-class <*name*> in

Use the **sip access-class in** command to limit the traffic allowed to reach the Session Initiation Protocol (SIP) stack by applying access control lists (ACLs) to incoming connections. Use the **no** form of this command to disable this feature. Variations of this command include:

sip access-class ip <*name*> **in**
sip access-class ipv6 <*name*> **in**

Syntax Description

ip	Specifies an Internet Protocol version 4 (IPv4) ACL.
ipv6	Specifies an Internet Protocol version 6 (IPv6) ACL.
<*name*>	Specifies the name of a previously configured ACL to apply to incoming traffic.

Default Values

By default, no ACL is configured or applied, and all traffic reaches the SIP stack.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to relocate the **ip** keyword and add the **ipv6** keyword.

Functional Notes

The **sip access-class in** command can be entered multiple times to apply multiple ACLs to incoming traffic to the SIP stack.

For more information regarding ACL configuration, refer to the *IPv4 Access Control List Command Set on page 4252* and *IPv6 Access Control List Command Set on page 4296*.

Usage Examples

The following example specifies an IPv4 SIP ACL name of **HSV**:

(config)**#sip access-class ip HSV in**

sip authenticate

Use the **sip authenticate** command to enable the Session Initiation Protocol (SIP) server authentication. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, the SIP server authentication is disabled.

Command History

Release 9.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example enables the SIP server authentication:

(config)**#sip authenticate**

sip database local

Use the **sip database local** command to store the location database of Session Initiation Protocol (SIP) user agents (UAs) across a power loss using memory on the local router. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 11.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example specifies storing the location database on the local router:

(config)**#sip database local**

sip default-call-routing

Use the **sip default-call-routing** command to specify the method used to route a call in the internal transaction distribution unit (TDU) when the destination of a call is ambiguous. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip default-call-routing proxy
sip default-call-routing reject
sip default-call-routing switchboard

Syntax Description

proxy	Specifies that the call is routed to a proxy server.
reject	Specifies that the call is rejected.
switchboard	Specifies that the call is routed to an internal switchboard.

Default Values

By default, the call routing method is **proxy**.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip default-call-routing** command is applicable to AOS voice products only. This command is not available on AOS data products.

Usage Examples

The following example specifies that calls are routed to an internal switchboard:

(config)**#sip default-call-routing switchboard**

sip grammar

Use the **sip grammar** command to populate privacy lists, indicating how caller ID is handled. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar default-privacy critical
sip grammar default-privacy header
sip grammar default-privacy none
sip grammar default-privacy session
sip grammar default-privacy user
sip grammar restricted-privacy critical
sip grammar restricted-privacy header
sip grammar restricted-privacy none
sip grammar restricted-privacy session
sip grammar restricted-privacy user

Syntax Description

default-privacy	Specifies entries into the default-privacy list for unrestricted caller ID calls.
restricted-privacy	Specifies entries into the restricted-privacy list for restricted caller ID calls.
critical	Adds critical to the Privacy header format. At least one other entry must be added to the list when using this setting.
header	Adds header to the Privacy header format.
none	Adds none to the Privacy header format. No other entries can be added to the list when using this setting.
session	Adds session to the Privacy header format.
user	Adds user to the Privacy header format.

Default Values

By default, both privacy lists are empty.

Command History

Release 13.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example sets all calls to have session privacy:

(config)**#sip grammar default-privacy session**

sip grammar alert-info url *<url>*

Use the **sip grammar alert-info url** command to specify the Alert-Info header host in outbound Session Initiation Protocol (SIP) messages. Use the **no** form of this command to return to the default setting.

Syntax Description

<url>	Specifies an Hypertext Transfer Protocol (HTTP) uniform resource locator (URL) to be used in the Alert-Info header for IP phone tone.

Default Values

By default, the local loopback address is the host in the Alert-Info header (127.0.0.1).

Command History

Release 13.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example sets the Alert-Info header to use a specific URL as shown in the sample header below:

(config)**#sip grammar alert-info url www.notused.com**

Sample header:

Alert-Info:<http://www.notused.com>;info=alert-internal

sip grammar contact host local

Use the **sip grammar contact host local** command to configure the Contact header on Session Initiation Protocol (SIP) messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar contact host local
sip grammar contact host local fqdn

Syntax Description

host local	Specifies that the local IP is used in the SIP Contact header.
fqdn	Optional. Specifies that a fully qualified domain name (FQDN) is used in the SIP Contact header.

Default Values

By default, SIP Contact headers use a local IP.

Command History

Release R13.11.0	Command was introduced.

Usage Examples

The following example specifies that AOS device should use a FQDN in the Contact header of SIP messages:

(config)**#sip grammar contact host local fqdn**

sip grammar contact host port persistent

Use the **sip grammar contact host port persistent** command to configure the AOS device to use the Transmission Control Protocol (TCP) port from which AOS initiated a Transport Layer Security (TLS) connection in the Contact uniform resource identifier (URI) sent by AOS. Use the **no** form of this command to disable this feature.

Syntax Description

host	Specifies the Contact header Host field setting.
port	Specifies the Contact header host port.
persistent	Specifies that the persistent connection port should be used for the Contact header host port.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced

Functional Notes

This configuration is useful when using client-only authentication. With this type of authentication, a persistent connection is established to the SIP server. Many SIP servers and enterprise session border controllers (eSBCs) need to see the TCP port from which AOS initiated the TLS connection in the Contact URI sent by AOS.

Usage Examples

The following example specifies that AOS device should use the TCP port from which AOS initiated the TLS connection in the Contact URI sent by AOS:

(config)**#sip grammar contact host port persistent**

sip grammar from

Use the **sip grammar from** command to configure the From header on Session Initiation Protocol (SIP) messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar from host domain
sip grammar from host local
sip grammar from host local fqdn
sip grammar from host override registered-users domain
sip grammar from host override registered-users local
sip grammar from host override registered-users sip-server
sip grammar from host sip-server
sip grammar from user domestic
sip grammar from user domestic <*Txx*>
sip grammar from user international
sip grammar from user international <*Txx*>

Syntax Description

host	Specifies the Host field formatting.
domain	Specifies the Domain for formatting the header.
local	Specifies the Local IP for formatting the header.
fqdn	Optional. Specifies a fully qualified domain name (FQDN) is used for formatting the header.
override registered-users	Overrides the current **sip grammar from host** setting for SIP messages originating from registered users.
sip-server	Specifies the SIP server for formatting the header.
user	Specifies the User field formatting.
domestic	Sends the number as specified by the calling party.
international	Sends the number with E.164 formatting.
<*Txx*>	Optional. Indicates a two-digit trunk identifier (i.e., T01).

Default Values

By default, the host for formatting messages is **sip-server**. Also, the default for the user format is **domestic**.

Command History

Release 11.1	Command was introduced.
Release 13.1	Command was expanded to include the domestic and international formats for the From User header.
Release A5.01	Command was expanded to include the **override registered-users** parameter.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Release R13.11.0	Command was expanded to include the **fqdn** parameter.

Functional Notes

Omitting the trunk option when issuing the **sip grammar from user** command specifies the User header globally.

Usage Examples

The following example sets the From header format to use a local IP:

(config)**#sip grammar from host local**

The following example sets the From header format to use calling party format on trunk **T02**:

(config)**#sip grammar from user domestic T02**

Technology Review

This technology review provides information about the E.164 recommendation for International numbering plans and telephone number formats.

A fully specified telephone number can have a maximum of 15 digits, including country code, area code, and the subscriber's number. These numbers usually consist of a + prefix. E.164 numbers exclude dialing prefixes. The most familiar prefixes are international direct dialing (IDD) and national direct dialing (NDD). In countries other than the USA, the IDD and NDD are represented by different numbers.

Additionally, E.123 describes the use of + to indicate a fully specified international number. The + is used in SIP headers to provide consistency across national and international phone calls.

AOS products provide support for E.164 by being able to specify a country code and an IDD prefix. National format telephone numbers are converted to international format by prefixing them with + and the country code. On outbound international calls, + is substituted for the IDD. On incoming international calls, the + is removed. If the country code matches the configured value, it too is removed.

*Setting the From header to **international** will cause phone numbers to be formatted as indicated by E.164. The country code must be configured, and the number must be of type **national** for this feature to work successfully.*

sip grammar p-asserted-identity host

Use the **sip grammar p-asserted-identity host** command to enable and format the private extensions to Session Initiation Protocol (SIP) for asserted identity within trusted networks. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar p-asserted-identity host domain
sip grammar p-asserted-identity host local
sip grammar p-asserted-identity host local fqdn
sip grammar p-asserted-identity host sip-server

Syntax Description

domain	Specifies the domain host for formatting the header.
local	Specifies the local IP as host for formatting the header.
fqdn	Optional. Specifies a fully qualified domain name (FQDN) is used for formatting the header.
sip-server	Specifies the SIP server as host for formatting the header.

Default Values

By default, the host for formatting messages is **sip-server**.

Command History

Release 13.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.
Release R13.11.0	Command was expanded to include the **fqdn** parameter.

Usage Examples

The following example sets the P-Asserted-Identity to use a local IP:

(config)**#sip grammar p-asserted-identity host local**

sip grammar p-early-media supported

Use the **sip grammar p-early-media supported** command to enable sending a P-Early-Media header with a value of "supported" in Session Initiation Protocol (SIP) INVITE, PRACK, and UPDATE requests. Use the **no** form of this command to disable the early media detection feature.

Syntax Description

No subcommands.

Default Values

By default, sending of the P-Early-Media header is disabled.

Command History

Release 13.6.0	Command was introduced.

Functional Notes

Support for sending the P-Early-Media header can be configured globally, using the **sip grammar p-early-media supported** command described here, or it can be configured on a per-trunk basis, using the command *grammar p-early-media supported on page 5076*. The trunk setting will always take precedence over the globally configured setting.

Usage Examples

To enable sending the P-Early-Media header, enter the command as follows:

(config)**#sip grammar p-early-media supported**

sip grammar proxy-require privacy

Use the **sip grammar proxy-require privacy** command to add a proxy-require header to Session Initiation Protocol (SIP) message packets containing a privacy header. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 13.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example allows a proxy-require header to be added to packets containing a privacy header:

(config)**#sip grammar proxy-require privacy**

sip grammar refer-to

Use the **sip grammar refer-to** command to configure the Session Initiation Protocol (SIP) Refer-To header on intratrunk attended transfers. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar refer-to intratrunk-attended-transfer source contact
sip grammar refer-to intratrunk-attended-transfer source to-from

Syntax Description

intratrunk-attended-transfer source	Configures the source for Refer-To header of an intratrunk attended transfer.
contact	Specifies the Contact header as the source for the Refer-To header.
to-from	Specifies either the To or From header as the source for Refer-To header.

Default Values

By default, the To or From header is the source for the Refer-To header on intratrunk attended transfers.

Command History

Release A5.01	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example specifies the Contact header as the source for the Refer-To header of an intratrunk attended transfer:

(config)**#sip grammar refer-to intratrunk-attended-transfer source contact**

sip grammar request-uri

Use the **sip grammar request-uri** command to format the Request uniform resource identifier (URI) for Session Initiation Protocol (SIP) messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar request-uri host domain
sip grammar request-uri host sip-server
sip grammar request-uri host-resolve
sip grammar request-uri transmit-network-selection <*parameter name*>

Syntax Description

host domain	Specifies the domain for formatting the header.
host sip-server	Specifies the SIP server IP for formatting the header.
host-resolve	Enables the local unit to resolve the domain before resolving the request URI.
transmit-network-selection <*parameter name*>	Specifies that Transmit Network Selection is included in the request URI.

Default Values

By default, the host for formatting messages is the SIP server. Also by default, **host-resolve** is disabled.

Command History

Release 11.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.
Release R13.8.0	Command was expanded to include the **transmit-network-selection** parameter.

Usage Examples

The following example enables SIP messages to resolve the request URI from the host domain:

(config)**#sip grammar request-uri host domain**

The following example enables SIP messages to resolve the request URI from the local unit:

(config)**#sip grammar request-uri host-resolve**

sip grammar require 100rel

Use the **sip grammar require 100rel** command to add **100rel** to the Require header of a Session Initiation Protocol (SIP) provisional response. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, **sip grammar require 100rel** is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

This command enables or disables the sending of reliable provisional responses to clients that *support* 100rel. Reliable provisional responses will always be sent to clients that *require* 100rel even with **sip grammar require 100rel** disabled.

Usage Examples

The following example enables **sip grammar require 100rel**:

(config)**#sip grammar require 100rel**

Technology Review

There are two Require headers that may use the 100rel tag, one in the initial request, and one in the provisional response.

The user agent client (UAC) is used to initiate SIP requests. When the UAC creates a new request, it can require reliable provisional responses for that request by adding the option tag 100rel to the Require header of that request.

The user agent server (UAS) contacts the user when SIP requests are received, and returns responses on behalf of the user, using provisional responses for request progress information. Provisional responses (100 to 199) are transmitted on a best-effort basis. By using reliable provisional responses, responses are sent by the UAS until they are acknowledged as received. This is especially beneficial when sending provisional responses over an unreliable transport, such as User Datagram Protocol (UDP).

The UAS must send any non-100 provisional responses reliably if the initial request contained a Require header field with the option tag 100rel. If the UAS is unwilling to do so, it must reject the initial request with a Bad Extension message and include an Unsupported header field containing the option tag 100rel. If the client *supports* 100rel, the UAS has the *option* of sending provisional responses with or without the Require 100rel tag as instructed by the **sip grammar require 100rel** command.

sip grammar supported 100rel

Use the **sip grammar supported 100rel** command to include 100rel in the supported header of the Session Initiation Protocol (SIP) message. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, **sip grammar supported 100rel** is disabled.

Command History

Release 14.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example enables **sip grammar supported 100rel**:

(config)**#sip grammar supported 100rel**

sip grammar to host

Use the **sip grammar to host** command to format the host format of the To header of a Session Initiation Protocol (SIP) message. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar to host domain
sip grammar to host sip-server

Syntax Description

domain	Specifies the domain for formatting the header.
sip-server	Specifies the SIP server for formatting the header.

Default Values

By default, the host for formatting messages is the SIP server.

Command History

Release 11.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example sets the To header format to use a domain host:

(config)**#sip grammar to host domain**

sip grammar user-agent

Use the **sip grammar user-agent** command to configure the user agent (UA) header format in Session Initiation Protocol (SIP) messages. The UA header can be given the default value for the product, a user-defined value, or no value at all, in which case the UA header is not sent in SIP messages. In addition, other specific values can be included in the UA header. Use the **no** form of this command to return to the default of the product. Variations of this command include the following:

sip grammar user-agent <*word*>
sip grammar user-agent default
sip grammar user-agent include custom-text <*word*>
sip grammar user-agent include firmware-version
sip grammar user-agent include hostname
sip grammar user-agent include serial-number
sip grammar user-agent none

Syntax Description

<*word*>	Specifies a word as a user-defined value to replace the default UA value. Maximum 128 letters.
default	Returns the UA header field to the default value.
include	Specifies that additional information is included in the UA header.
custom-text <*word*>	Specifies that a user-defined value is included in the UA header. Maximum 128 letters.
firmware-version	Specifies that the firmware version is included in the UA header.
hostname	Specifies that the host name is included in the UA header.
serial-number	Specifies that the serial number is included in the UA header.
none	Disables the UA header field resulting in no UA header sent in SIP messages.

Default Values

By default, the UA value is set to the default value of the product.

Command History

Release 15.1	Command was introduced.
Release R10.3.0	Command was expanded to include the **include** parameters.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example removes the UA header field from SIP messages:

(config)**#sip grammar user-agent none**

sip hmr

Use the **sip hmr** command to apply a Session Initiation Protocol (SIP) header manipulation rule (HMR) policy to all SIP traffic on the AOS device. Use the **no** form of this command to remove the HMR policy. Variations of this command include:

sip hmr <*name*> **in**
sip hmr <*name*> **out**

Syntax Description

<*name*>	Specifies the name of the HMR policy to apply to the SIP traffic.
in	Specifies that the HMR policy is applied to ingress SIP traffic.
out	Specifies that the HMR policy is applied to egress SIP traffic.

Default Values

By default, no SIP HMR policies are applied to SIP traffic.

Command History

Release R10.1.0	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

For more information about SIP HMR and its uses and configuration, refer to the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example adds the HMR policy **MYPOLICY1** to the AOS unit for all inbound SIP traffic:

(config)**#sip hmr MYPOLICY1 in**

sip inbound-trunk-matching

Use the **sip inbound-trunk-matching** command to enable and configure inbound trunk matching. Use the **no** form of this command to return to the default settings. Variations of this command include:

sip inbound-trunk-matching default-trunk <*Txx*>
sip inbound-trunk-matching prefer trunk-routing
sip inbound-trunk-matching require-registration

Syntax Description

default-trunk <*Txx*>	Specifies a trunk to use when matching fails. The trunk is specified in the format Txx (e.g., **T01**).
prefer trunk-routing	Specifies that trunk matches are preferred over users.
require-registration	Indicates that the request uniform resource identifier (URI) user is required to be registered on a trunk.

Default Values

By default, there is no default trunk set and the **require-registration** option is disabled.

Command History

Release A2.03	Command was introduced.
Release A4.01	Command was expanded to include the **prefer trunk-routing** parameter.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example configures AOS to require registration for inbound trunk matching:

(config)**#sip inbound-trunk-matching require-registration**

sip location

Use the **sip location** command to manually add a Session Initiation Protocol (SIP) user agent (UA) to the location database. Use the **no** form of this command to disable this feature. Variations of this command include:

sip location *<username> <ip address>*
sip location *<username> <ip address> <port>*
sip location *<username> <ip address> <port>* **tcp**
sip location *<username> <ip address> <port>* **tcp** *<number>*
sip location *<username> <ip address> <port>* **udp**
sip location *<username> <ip address> <port>* **udp** *<number>*

Syntax Description

<username>	Specifies the user name for the UA being added to the location database.
<ip address>	Specifies the IP address for the UA being added to the location database. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).
<port>	Optional. Specifies the port of the UA to add to the database. If no port is specified, default port is **5060**.
tcp	Optional. Specifies the use of Transmission Control Protocol (TCP) for session communication.
udp	Optional. Specifies the use of User Datagram Protocol (UDP) for session communication.
<number>	Optional. Specifies the time in seconds that a user is stored in the database. Range from **0** to **36000**. If no time is specified, default time is zero seconds.

Default Values

By default, this command is disabled.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was expanded to include a choice of transport protocols and expiration time.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example specifies an IPv4 SIP location of **192.33.5.99** for a user named **2001**:

(config)**#sip location 2001 192.33.5.99**

sip prefer double-reinvite

Use the **sip prefer double-reinvite** command to specify globally that Session Initiation Protocol (SIP) double reInvite messages are included in calls in the system. Calls that typically require a double reInvite are forwarded calls from call overage and any attended transfer, and when these calls connect, a double reInvite message is initiated when the feature is enabled. Using the **no** form of this command indicates that double reInvites are not globally preferred. Use the commands *prefer double-reinvite on page 5113* and *prefer reinvite-without-sdp on page 5114* to specify the trunk settings for this feature.

This command should only be issued by advanced users or at the direction of Adtran technical support.

Syntax Description

No subcommands.

Default Values

By default, all calls in the system prefer a double reInvite.

Command History

Release A5.01	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip prefer double-reinvite** command is used in the Global Configuration mode to determine whether a double reInvite is preferred in calls in the system. By default, the system is configured so that double reInvites are preferred, and all trunk accounts prefer a double reInvite. Double reInvites are used, for example, when a SIP trunk in local transfer mode is providing ring-back during a blind transfer. In this scenario, a double reInvite must occur in order to establish a talk path after the transfer target answers.

You can specify whether a specific trunk prefers a double reInvite by using the command *prefer double-reinvite on page 5113*.

You can also specify whether Session Description Protocol (SDP) is used in the double reInvite message. To send a double reInvite without SDP, refer to the command *prefer reinvite-without-sdp on page 5114*. When a double reInvite is initiated, the first reInvite without SDP is not sent to the account that does not require it. When both accounts do not require a reInvite with SDP, the target account sends the initial reInvite message.

Usage Examples

The following example specifies that SIP double reInvites are not preferred in the system:

(config)**#no sip prefer double-reinvite**

sip privacy

Use the **sip privacy** command to specify outbound calls to include privacy headers (when configured) and inbound calls to be filtered on privacy settings. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, Session Initiation Protocol (SIP) privacy is disabled.

Command History

Release 13.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example enables SIP privacy:

(config)**#sip privacy**

sip proxy

Use the **sip proxy** command to enable Stateful and Outbound modes of Session Initiation Protocol (SIP) proxy operation at the global level. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

Although the **sip proxy** command enables Stateful and Outbound modes of SIP proxy operation, it is also necessary to use this command in conjunction with the **sip proxy transparent** command for transparent proxy mode. For more information about transparent proxy, refer to the command *sip proxy transparent on page 1764*.

For more information about SIP proxy, refer to the *Configuring SIP Proxy in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example allows the SIP proxy server to operate in the Stateful and Outbound modes:

(config)**#sip proxy**

sip proxy allowed-servers <*hostname* | *ip address*>

Use the **sip proxy allowed-servers** command to specify a server to which devices behind the proxy are allowed to send Session Initiation Protocol (SIP) traffic. Use the **no** form of this command to return to the default setting.

Syntax Description

<*hostname* | *ip address*>	Specifies the fully qualified domain name (FQDN) or IP address of the SIP proxy server. IPv4 addresses should be expressed in dotted decimal notation (for example, **208.61.209.1**). IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).

Default Values

By default, SIP traffic to any server is allowed in Transparent and Outbound proxy modes. This means that if no server is specified, traffic to any server is permitted, but if this command is entered, only traffic to the configured servers is allowed.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip proxy allowed-servers** command can be entered multiple times to allow traffic to multiple servers.

Usage Examples

The following example adds the server with an IPv4 address of **10.200.1.9** as an allowed SIP proxy server:

(config)**#sip proxy allowed-servers 10.200.1.9**

sip proxy dial-string source

Use the **sip proxy dial-string source** command to specify the dial-string source for the Session Initiation Protocol (SIP) proxy server. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip proxy dial-string source request-uri
sip proxy dial-string source to

Syntax Description

request-uri	Specifies the Request-URI user field as the dial-string source.
to	Specifies the To header as the dial-string source.

Default Values

By default, the dial-string source is set to **request-uri**.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example sets the To header as the dial-string source:

(config)**#sip proxy dial-string source to**

sip proxy domain *<string>*

Use the **sip proxy domain** command to specify a domain string for Session Initiation Protocol (SIP) proxy messaging. Use the **no** form of this command to return to the default setting.

Syntax Description

<string>	Specifies the domain string for SIP messaging.

Default Values

By default, **sip proxy domain** is not configured.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example specifies **Sample** as the SIP proxy domain string:

(config)**#sip proxy domain Sample**

sip proxy emergency-call-routing

Use the **sip proxy emergency-call-routing** command to first specify the Session Initiation Protocol (SIP) proxy method used to route a call during failover and to then specify the calls that are considered emergency calls for SIP proxy emergency routing. Use the **no** form of this command to disable emergency call routing and to remove the call routing templates. Variations of this command include:

sip proxy emergency-call-routing local
sip proxy emergency-call-routing proxy
sip proxy emergency call-routing accept *<template>*
sip proxy emergency-call-routing reject *<template>*

Syntax Description

local	Specifies that all emergency calls are routed directly through the switchboard.
proxy	Specifies that all emergency calls are routed through the proxy before sending them to the switchboard.
accept *<template>*	Specifies that calls matching the template are accepted as emergency calls. Refer to the Functional Notes section of this command for more information.
reject *<template>*	Specifies that calls matching the template are rejected as emergency calls. Refer to the Functional Notes section of this command for more information.

Default Values

By default, the SIP proxy is set to send all emergency calls directly through the switchboard (the **local** parameter). By default, no emergency number templates or patterns are configured in the system; therefore, no calls are classified as emergency calls.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

Before specifying which calls are defined as emergency calls, you should configure the method used for routing emergency calls (using the **sip proxy emergency-call-routing local** or **sip proxy emergency-call-routing proxy** commands). For the default emergency call routing method (**local**) to function on AOS data products, a local SIP gateway must be configured using the command *sip proxy local-gateway <hostname | ip address> on page 1751*. On AOS voice products, the local SIP gateway is enabled by default.

After the emergency call routing method has been specified, emergency calls must be defined for emergency call routing to perform any action. Emergency call definitions are configured using the **sip proxy emergency-call routing accept** *<template>* and **sip proxy emergency-call-routing reject** *<template>* commands.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example enables SIP proxy emergency call routing on an AOS voice product and specifies the routing method as **proxy**:

(config)**#sip proxy emergency-call-routing proxy**

The following example specifies a local SIP gateway and enables SIP proxy emergency call routing on an AOS data product:

(config)**#sip proxy local-gateway 10.19.209.55**
(config)**#sip proxy emergency-call-routing local**

The following example specifies that 911 calls are accepted as emergency calls on an AOS voice product:

(config)**#sip proxy emergency-call-routing proxy**
(config)**#sip proxy emergency-call-routing accept 911**

The following example specifies that 911 calls are accepted as emergency calls on an AOS data product:

(config)**#sip proxy local-gateway 10.19.209.55**
(config)**#sip proxy emergency-call-routing local**
(config)**#sip proxy emergency-call-routing accept 911**

sip proxy failover accept-registrations

Use the **sip proxy failover accept-registrations** command to configure the Session Initiation Protocol (SIP) proxy server to accept new registrations when the system is in survivability (failover) mode. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release A2.03	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example enables the server to accept registration during failover conditions:

(config)**#sip proxy failover accept-registrations**

sip proxy failover codec-group <*name*>

Use the **sip proxy failover codec-group** command to specify the Session Initiation Protocol (SIP) proxy server's coder-decoder (CODEC) when the system is in failover mode. Use the **no** form of this command to return to the default setting.

Syntax Description

<*name*>	Specifies the name of a previously created CODEC list to be used during failover.

Default Values

By default, no CODEC list is configured or applied.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip proxy failover codec-group** command is available on AOS voice products only. This command is not available on AOS data products. For more information regarding CODEC list configuration, refer to the *Voice CODEC List Command Set on page 4893*.

For more information regarding SIP proxy configuration, refer to the *Configuring SIP Proxy in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables the CODEC list named **List1** during failover:

(config)**#sip proxy failover codec-group List1**

sip proxy failover dial-string source

Use the **sip proxy failover dial-string source** command to specify the dial-string source for the Session Initiation Protocol (SIP) proxy server when the system is in survivability (failover) mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip proxy failover dial-string source request-uri
sip proxy failover dial-string source to

Syntax Description

request-uri	Specifies the Request-URI user field as the dial-string source.
to	Specifies the To header as the dial-string source.

Default Values

By default, the dial-string source is **request-uri**.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example specifies using the To header for the dial-string source:

(config)**#sip proxy failover dial-string source to**

sip proxy failover direct-inbound

Use the **sip proxy failover direct-inbound** command to allow direct inbound routing of calls to proxy users during failover mode without first routing the call out a Session Initiation Protocol (SIP) trunk. This feature is used when a network configuration does not use a SIP trunk. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, direct inbound call routing is disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables direct inbound routing of calls during failover:

(config)**#sip proxy failover direct-inbound**

sip proxy failover group match-value <*pattern*> new-value <*pattern*>

Use the **sip proxy failover group match-value new-value** command to enable forking of calls to users registered with unique extensions in survivability (failover) mode. Use the **no** form of this command to return to remove the entry.

The following configurations can lead to unexpected behavior:

- *Matching a valid extension with multiple groups.*
- *Creating a failover group with an existing extension.*

Syntax Description

<pattern>	Specifies a number pattern using either traditional number matching or regular expression matching methods. Refer to the *Functional Notes* below for more information.

Default Values

By default, there are no failover group patterns defined.

Command History

Release R11.6.0	Command was introduced.

Functional Notes

For more information about configuring SIP proxy failover, refer to the *Configuring SIP Proxy in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Both the **match-value** <*pattern*> and the **new-value** <*pattern*> parameters can be defined using traditional number matching and regular expression matching methods. Traditional number matching uses numbers and wildcard variables to enter a pattern.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

In regular expressions number matching, the match strings are encapsulated by paired */* (slash) symbols. This indicates that the pattern is to be treated as a regular expression. Using regular expressions allows greater flexibility in matching multiple number templates with fewer expressions.

NOTE *AOS is compatible with Perl compatible regular expressions (PCREs). More information on understanding and using regular expressions is available at* http://www.pcre.org.

NOTE *The use of quotation marks in a command syntax, when entering a string is not necessary unless the string requires using a space or* **?***. Using either of these characters outside of quotation marks is interpreted by the CLI as commands and not recognized as part of the string. The use of quotation marks in the following examples are provided to cover all possible user-entered strings. These examples can be entered without the quotation marks and function in the same manner.*

Usage Examples

The following example uses the regular expression number matching method to match a dial string beginning with **5551111.sca** and create a failover group that can be dialed as **5551111**:

(config)**#sip proxy failover group match-value "/^5551111\.sca/" new-value "/5551111/"**

sip proxy failover match-alias <*pattern*> substitute <*pattern*>

Use the **sip proxy failover match-alias substitute** command to configure an alias to match a dial string and substitute the specified pattern. This feature is used to route a survivability call when the Session Initiation Protocol (SIP) proxy is in failover mode. If an INVITE message is directed toward a matching alias, the substitution pattern is evaluated and compared to current proxy users. The first user to match the substitution pattern is selected to receive the SIP message. Use the **no** form of this command to return to the default setting.

Syntax Description

<*pattern*>	Specifies a number pattern using either traditional number matching or regular expression matching methods. Refer to the *Functional Notes* below for more information.

Default Values

By default, there are not match-alias substitutions defined.

Command History

Release A4.05	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

SIP proxy failover occurs using an automatically created trunk contained in AOS's basic configuration. This trunk is a hidden SIP trunk with the same default settings as a regular SIP trunk. For more information about configuring SIP proxy failover, refer to the *Configuring SIP Proxy in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Both the **match-alias** <*pattern*> and the **substitute** <*pattern*> parameters can be defined using traditional number matching and regular expression matching methods. Traditional number matching uses numbers and wildcard variables to enter a pattern.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

In regular expressions number matching, the match strings are encapsulated by paired **/** (slash) symbols. This indicates that the pattern is to be treated as a regular expression. Using regular expressions allows greater flexibility in matching multiple number templates with fewer expressions.

NOTE

AOS is compatible with Perl compatible regular expressions (PCREs). More information on understanding and using regular expressions is available at http://www.pcre.org.

NOTE

The use of quotation marks in a command syntax, when entering a string is not necessary unless the string requires using a space or **?***. Using either of these characters outside of quotation marks is interpreted by the CLI as commands and not recognized as part of the string. The use of quotation marks in the following examples are provided to cover all possible user-entered strings. These examples can be entered without the quotation marks and function in the same manner.*

Usage Examples

The following example uses the traditional number matching method to match a 7-digit number beginning with **555** and replace it with **5551111**:

(config)**#sip proxy failover match-alias “555XXXX” substitute “5551111”**

The following example uses the regular expression number matching method to match a 7-digit number beginning with **555** and replace it with **5551111**:

(config)**#sip proxy failover match-alias “/555\d{4}/” substitute “/5551111/”**

sip proxy failover match-digits *<value>*

Use the **sip proxy failover match-digits** command to specify the number of least-significant digits of the dial string to match in order to route a surviving call to proxy users during when in failover mode. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the number of digits within a template to match during failover. The valid range is **1** to **255**.

Default Values

By default, the number of **match-digits** is not specified.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip proxy failover match-digits** command can be entered multiple times.

Session Initiation Protocol (SIP) proxy failover occurs using an automatically created trunk contained in AOS's basic configuration. This trunk is a hidden SIP trunk with the same default settings as a regular SIP trunk. For more information about configuring SIP proxy failover, refer to the *Configuring SIP Proxy in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example sets the **sip proxy failover match-digits** to **7**:

(config)**#sip proxy failover match-digits 7**

sip proxy failover register-expires <*value*>

Use the **sip proxy failover register-expires** command to specify the length of time Session Initiation Protocol (SIP) phone registrations remain in the SIP Proxy database while in failover mode. Once the **register-expires** time has elapsed, the SIP phones must re-register or they will be removed from the SIP Proxy database. This setting only applies when the SIP Proxy is in failover mode. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the amount of time (in seconds) that the registration is valid. Time range is **30** to **86400** seconds.

Default Values

By default, the registration value is 300 seconds.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example specifies the failover registration is valid for 120 seconds:

(config)**#sip proxy failover register-expires 120**

sip proxy failover sip-keep-alive

Use the **sip proxy failover sip-keep-alive** command to configure the Session Initiation Protocol (SIP) proxy server keep-alive method when the system is in survivability (failover) mode. Keep-alive messages must be sent between the SIP device and the registrar to keep the connected channel open for communication. Use the **no** form of this command to return to the default setting. Variations of this command include the following:

sip proxy failover sip-keep-alive info
sip proxy failover sip-keep-alive info <*value*>
sip proxy failover sip-keep-alive options
sip proxy failover sip-keep-alive options <*value*>

Syntax Description

<*value*>	Specifies the amount of time in seconds between keep-alive messages sent during a call. The range is **30** to **3600** seconds.
info	Specifies using the INFO keep-alive method on this trunk.
options	Specifies using the OPTIONS keep-alive method on this trunk.

Default Values

By default, this command is not configured.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example enables the INFO method to be used as the SIP keep-alive method with the timeout between messages set to 3 minutes:

(config)**#sip proxy failover sip-keep-alive info 180**

sip proxy failover trust-domain

Use the **sip proxy failover trust-domain** command to enable the AOS unit to use P-Asserted Identity Session Initiation Protocol (SIP) privacy when communicating with the softswitch when in failover mode. Use the **no** form of this command to disable this feature. Variations of this command include:

sip proxy failover trust-domain
sip proxy failover trust-domain p-asserted-identity-required

Syntax Description

p-asserted-identity-required	Specifies that P-Asserted-Identity is required for this domain.

Default Values

By default, this command is disabled.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip proxy failover trust-domain** command allows the AOS unit to look at any P-Asserted-Identity header the phones might send while the AOS device is in failover mode. The **p-asserted-identity-required** parameter is only used with nonstandard softswitches and should not be used in normal configurations.

Usage Examples

The following example specifies that P-Asserted-Identity is enabled:

(config)**#sip proxy failover trust-domain**

sip proxy force-port-translation

Use the **sip proxy force-port-translation** command to enable **force-port-translation** for Session Initiation Protocol (SIP) proxy operation. Enabling this feature allows a SIP user to register from multiple phones to the SIP Proxy. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip proxy force-port-translation
sip proxy force-port-translation exclude-via

This command has a very limited application and only applies to very specific network configurations. If you are not familiar with its usage, contact Adtran Technical Support for assistance.

Syntax Description

exclude-via	Indicates excluding the Via header from port translation.

Default Values

By default, this feature is disabled.

Command History

Release 17.9	Command was introduced for AOS data products.
Release A2.07	Command was included for AOS voice products.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

Enabling **force-port-translation** allows the SIP Proxy to create a unique registration in the user database for the same user from multiple phones. This feature retains the key generated by the proxy and inserted into the user portion of the Contact header. It also uses the source port that is generated by the firewall when doing NAT. The source port is inserted at the end of the host portion of any address translated in the SIP header. Enabling the **exclude-via** parameter on this command, excludes the Via header from the source port translation.

Usage Examples

The following example enables **force-port-translation**:

(config)**#sip proxy force-port-translation**

sip proxy grammar

Use the **sip proxy grammar** command to specify the Session Initiation Protocol (SIP) proxy grammar options. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip proxy grammar contact outbound-server-reference host domain
sip proxy grammar contact outbound-server-reference host sip-server
sip proxy grammar expires param-conversion
sip proxy grammar non-invite domain-undo
sip proxy grammar from host domain
sip proxy grammar from host sip-server
sip proxy grammar request-uri host domain
sip proxy grammar request-uri host sip-server
sip proxy grammar to host domain
sip proxy grammar to host sip-server

Syntax Description

expires param-conversion	Enables conversion of Expires parameters to Expires headers.
non-invite domain-undo	Enables translation of domain address to proxy address for inbound stateful requests.
from	Configures grammar for the From header.
request-uri	Configures grammar for the Request URI header.
to	Configures grammar for the To header.
host	Configures the host portion of the specified header.
domain	Specifies using the configured domain string in the specified header.
sip-server	Specifies using the resolved SIP server address in the specified header.
contact	Configures grammar for the Contact header.
outbound-server-reference	Configures the Contact header grammar for outbound server references**.**

Default Values

By default, **sip proxy grammar** for all option headers is **sip-server**.

Command History

Release 16.1	Command was introduced.
Release 17.3	Command was expanded to include the Expires header option.
Release A2	Command was expanded to include the Non-Invite header option.
Release A5.01	Command was expanded to include the Contact header option and **outbound-server-reference** parameter.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example configures the To header using the configured SIP proxy domain string:

(config)**#sip proxy grammar to host domain**

sip proxy hmr

Use the **sip proxy hmr** command to apply a Session Initiation Protocol (SIP) header manipulation rule (HMR) policy to SIP traffic to or from devices (such as phones) behind a SIP proxy or to SIP proxy traffic travelling to or from proxy servers. Use the **no** form of this command to remove the HMR policy. Variations of this command include:

sip proxy hmr server <*name*> **in**
sip proxy hmr server <*name*> **out**
sip proxy hmr user <*name*> **in**
sip proxy hmr user <*name*> **out**

Syntax Description

<*name*>	Specifies the name of the HMR policy to apply to the SIP traffic.
server	Specifies that the HMR policy is applied to SIP traffic to or from SIP proxy servers.
user	Specifies that the HMR policy is applied to SIP traffic to or from devices behind the SIP proxy (such as phones).
in	Specifies the HMR policy is applied to ingress traffic.
out	Specifies the HMR policy is applied to egress traffic.

Default Values

By default, no SIP HMR policies are applied to SIP traffic.

Command History

Release R10.1.0	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

For more information about SIP HMR and its uses and configuration, refer to the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example adds the HMR policy **MYPOLICY1** for all inbound SIP proxy user traffic:

(config)**#sip hmr proxy user MYPOLICY1 in**

The following example adds the HMR policy **MYPOLICY1** for all inbound SIP proxy server traffic:

(config)**#sip hmr proxy server MYPOLICY1 in**

sip proxy local-gateway <*hostname* | *ip address*>

Use the **sip proxy local-gateway** command to configure the local Session Initiation Protocol (SIP) gateway. Use the **no** form of this command to disable this feature. Variations of this command include:

sip proxy local-gateway <*hostname* | *ip address*>
sip proxy local-gateway <*hostname* | *ip address*> **tcp**
sip proxy local-gateway <*hostname* | *ip address*> **tcp** <*port*>
sip proxy local-gateway <*hostname* | *ip address*> **udp**
sip proxy local-gateway <*hostname* | *ip address*> **udp** <*port*>

Syntax Description

<*hostname* | *ip address*>	Specifies the host name or IP address of the local SIP proxy gateway. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).
tcp	Optional. Configures the gateway to use Transmission Control Protocol (TCP).
udp	Optional. Configures the gateway to use User Datagram Protocol (UDP).
<*port*>	Optional. Specifies the TCP or UDP port used by the gateway. Range is **1** to **65535**.

Default Values

By default, the **sip proxy local-gateway** is not configured. When configured, the default protocol is **udp** on port **5060**. If a particular protocol is configured and no port is specified, the default port is set to **5060**.

Command History

Release 17.3	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip proxy local-gateway** command enables the necessary local SIP gateway in AOS data products. This gateway is necessary for routing emergency calls when using SIP proxy. On AOS voice products, the local gateway is enabled by default.

Usage Examples

The following example sets the local gateway:

(config)**#sip proxy local-gateway serviceprovider@network.com**

sip proxy register rate-adaption

Use the **sip proxy register rate-adaption** command to configure REGISTER rate-adaption for Session Initiation Protocol (SIP) proxy users. This command allows you to reduce the rate that SIP proxy users' REGISTER requests are forwarded by the unit to the SIP server. Use the **no** form of this command to return to disable this feature. Variations of this command include:

sip proxy register rate-adaption
sip proxy register rate-adaption server-expires <*value*>
sip proxy register rate-adaption threshold absolute <*value*>
sip proxy register rate-adaption threshold percentage <*percentage*>
sip proxy register rate-adaption user-expires <*value*>

Syntax Description

server-expires <*value*>	Specifies the expiration period requested from the SIP server in the REGISTER request. Valid range is **30** to **86400** seconds.
threshold absolute <*value*>	Specifies a fixed amount of time that is used to determine when the unit will forward a REGISTER request from the SIP proxy user to the SIP server. The value of this parameter must be less than the value set by the **server-expires** <*value*> parameter. Valid range is **5** to **604800** seconds
threshold percentage <*percentage*>	Specifies a percentage of the REGISTER expiration period that is used to determine when the unit will forward a REGISTER request from the SIP proxy user to the SIP server. Valid range is **10** to **90** percent.
user-expires <*value*>	Specifies the expiration period (in seconds) given to the SIP proxy user in the REGISTER response. Valid range is **30** to **86400** seconds.

Default Values

The default **server-expires** value is **3600**. The default **user-expires** value is **60**. The default threshold is **threshold percentage 50**.

Command History

Release A5.02	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

This command allows the unit to reduce the load of REGISTER requests sent by SIP proxy users to the SIP server. When this command is enabled, the unit modifies the Expires header to be a large value in outbound REGISTER requests to the SIP server (defined by the **server-expires** <*value*> parameter). In the corresponding responses from the SIP server, the unit modifies the Expires header to be a small value when forwarding the REGISTER response to the phone (defined by the **user-expires** <*value*> parameter). The ratio between these two times determines how many REGISTER requests (after the first) the unit forwards to the SIP server and how many REGISTER requests the unit will handle locally. SIP proxy user REGISTER requests are forwarded by the unit if the time remaining in the REGISTER expiration period is less than or equal to the REGISTER expiration period received from the SIP server minus the threshold (defined by the **threshold absolute** <*value*> and **threshold percentage** <*percentage*> parameters) minus the modified REGISTER expiration period forwarded to the SIP proxy user. All other REGISTER requests from SIP proxy users are handled locally by the unit. For example, if the REGISTER expiration period from the SIP server is 3600 seconds, the threshold is set to **threshold absolute 180**, and the REGISTER expiration period in the modified REGISTER response forwarded to the user is 60 seconds, then the first REGISTER request from the SIP proxy user that occurs after 3360 seconds (3600 - 180 - 60) will be forwarded to the SIP server. Similarly, if the REGISTER expiration period from the SIP server is 3600 seconds, the threshold is set to **threshold percent 10**, and the modified Expires period in the REGISTER response given to the user is 60 seconds, then the first REGISTER request from the SIP proxy user that occurs after 3180 seconds (3600 - .10(3600) - 60) will be forwarded to the SIP server.

Usage Examples

The following example specifies a rate-adaption threshold of **10** percent of the Expires period from the SIP server:

(config)**#sip proxy register rate-adaption threshold percentage 10**

sip proxy routing contact-comparison strict

Use the **sip proxy routing contact-comparison strict** command to configure the Session Initiation Protocol (SIP) proxy server to make strict comparisons between Contact headers. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release A2.03	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example modifies the Contact comparison settings to make strict comparisons of Contact headers during routing:

(config)**#sip proxy routing contact-comparison strict**

sip proxy routing server-selection in-dialog

Use the **sip proxy routing server-selection in-dialog** command to configure the Session Initiation Protocol (SIP) server selection method used by the SIP proxy for new outbound SIP requests within an existing dialog. Use the **no** form of this command to return to the default setting.Variations of this command include the following:

sip proxy routing server-selection in-dialog configured
sip proxy routing server-selection in-dialog learned

Syntax Description

configured	Specifies that the SIP proxy uses configured SIP servers (in order) as the destination for new outbound SIP requests in an existing dialog.
learned	Specifies that the SIP proxy uses the SIP server learned from a given dialog as the destination for new outbound SIP requests in that dialog.

Default Values

By default, the SIP proxy server selection is set to **learned**.

Command History

Release R12.2.0	Command was introduced.

Usage Examples

The following example configures the SIP proxy to use previously configured SIP servers as the destination for new outbound SIP requests in an existing dialog:

(config)**#sip proxy routing server-selection in-dialog configured**

sip proxy sip-server monitor

Use the **sip proxy sip-server monitor** command to enable the Session Initiation Protocol (SIP) proxy server monitor feature and enter the SIP Proxy SIP-Server Monitor command set. Use the **no** form of this command to disable the feature and return to the default settings. For more information on commands available for configuring this feature, refer to *SIP Proxy Monitor Command Set on page 4866*.

Syntax Description

No subcommands.

Default Values

By default, **sip proxy sip-server monitor** is disabled.

Command History

Release R10.9.0	Command was introduced.

Functional Notes

The SIP proxy SIP server monitor feature adds rollover support to the SIP proxy in stateful mode. If the currently selected SIP server becomes unresponsive, the proxy uses a secondary proxy server for all future calls. The proxy monitor polls the failed SIP servers to detect when they are operational again. Calls are routed to more preferred servers as service is restored.

Usage Examples

The following example enables the **sip proxy sip-server monitor** and enters the SIP Proxy SIP-Server Monitor configuration mode:

```
(config)#sip proxy sip-server monitor
    Configuring New Proxy Monitor.
(config-proxy-monitor)#
```


sip proxy sip-server monitor stateful

Use the **sip proxy sip-server monitor stateful** command to enable the Session Initiation Protocol (SIP) proxy server monitor feature for transparent SIP proxy. Use the **no** form of this command to disable the feature and return to the default settings. Variations of this command include:

sip proxy sip-server monitor stateful-transparent
sip proxy sip-server monitor stateful-only

Syntax Description

stateful-transparent	Specifies that SIP monitor is enabled for stateful and transparent SIP proxy.
stateful-only	Specifies that SIP monitor is enabled for stateful SIP proxy only.

Default Values

By default, **sip proxy sip-server monitor** is set to **stateful-only**.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

This command sets the SIP monitor state for the transparent SIP proxy; it does NOT create a SIP proxy monitor for non-transparent proxy, or enter the monitor's configuration. The SIP monitor for non-transparent proxy configuration is available only using the command *sip proxy sip-server monitor on page 1756*.

When the transparent proxy monitor is enabled, it compares the destination SIP server in the SIP packet to the configured list of SIP servers. If the destination matches a server in the list, the proxy determines if any of the configured servers are UP. If at least one server is up, the transparent proxy does not go into failover mode, and the phone is expected to try another SIP server. If none of the monitored servers are UP, the proxy transitions the call to failover mode.

Usage Examples

The following example enables the SIP transparent proxy monitor:

(config)**#sip proxy sip-server monitor stateful-transparent**

sip proxy sip-server primary

Use the **sip proxy sip-server primary** command to configure the primary Session Initiation Protocol (SIP) server softswitch. Use the **no** form of this command to disable the softswitch. The softswitch cannot be disabled unless all configured secondary softswitches are removed (refer to the command *sip proxy sip-server secondary on page 1761*). Variations of this command include:

sip proxy sip-server primary *<hostname | ip address>*
sip proxy sip-server primary *<hostname | ip address>* **tcp**
sip proxy sip-server primary *<hostname | ip address>* **tcp** *<port>*
sip proxy sip-server primary *<hostname | ip address>* **tls** *<profile name>*
sip proxy sip-server primary *<hostname | ip address>* **tls** *<profile name> <TLS port>*
sip proxy sip-server primary *<hostname | ip address>* **tls** *<profile name> <TLS port>*
srv *<service-name-prefix>*
sip proxy sip-server primary *<hostname | ip address>* **tls** *<profile name> <TLS port>*
srv *<service-name-prefix> <transport-name-prefix>*
sip proxy sip-server primary *<hostname | ip address>* **tls** *<profile name>* **srv** *<service-name-prefix>*
sip proxy sip-server primary *<hostname | ip address>* **tls** *<profile name>* **srv** *<service-name-prefix>*
<transport-name-prefix>
sip proxy sip-server primary *<hostname | ip address>* **udp**
sip proxy sip-server primary *<hostname | ip address>* **udp** *<port>*

Syntax Description

<hostname | ip address>	Specifies the fully qualified domain name (FQDN) or IP address of the outbound SIP proxy server. IPv4 addresses should be expressed in dotted decimal notation (for example, **208.61.209.1**). IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).
tcp	Optional. Configures the softswitch to use Transmission Control Protocol (TCP).
<port>	Optional. Specifies the TCP port used by the softswitch. Range is **1** to **65535**.
tls *<profile name>*	Optional. Specifies the SIP traffic uses Transport Layer Security (TLS). If TLS is specified, a TLS profile must be specified. The TLS profile must have been created prior to issuing this command (refer to the command *tls-profile <profile name> on page 1885*).
<TLS port>	Optional. Specifies the TLS destination port. Range is **1** to **65535**.
srv *<service name prefix>*	Optional. Specifies the service name prefix for the DNS SRV request. Underscores are added automatically.
<transport-name-prefix>	Optional. Specifies the transport prefix for the DNS SRV request. Underscores are added automatically.
udp	Optional. Configures the softswitch to use User Datagram Protocol (UDP).
<port>	Optional. Specifies the UDP port used by the softswitch. Range is **1** to **65535**.

Default Values

By default, no softswitches are configured. If a softswitch is configured, the default protocol is UDP on port **5060**. If a particular protocol is configured and no port is specified, the default port is set to **5060**.

If TLS is used, port **5061** is used by default. By default, SIP TLS requests use **sips** as the service name prefix and **tcp** as the transport name prefix.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.
Release R13.1.0	Command was expanded to include the **tls** <*profile name*>, <*TLS port*>, and **srv** parameters.

Functional Notes

The guidelines for configuring the softswitch(es) depend on the mode of operation selected. Softswitch configuration is always needed for Stateful mode. It is only needed for Outbound mode and Transparent mode when the SIP Request does not contain any fields that can be resolved to the softswitch's location.

If a host name is used to specify the outbound SIP proxy server, a domain naming system (DNS) server must be configured on the AOS unit using the command *name-server on page 1622* or learned via a dynamic IP interface.

To configure the primary softswitch with a TLS profile, the TLS profile must have been created prior to issuing this command (refer to the command *tls-profile <profile name> on page 1885*). If a specified TLS profile is ever deleted, this softswitch is automatically removed from the AOS device's configuration. If the TLS profile specified by the primary softswitch is removed from the AOS device configuration, both the primary and all secondary softswitches are automatically removed from the AOS device configuration.

Usage Examples

The following example sets the primary softswitch:

(config)**#sip proxy sip-server primary 208.61.209.1**

sip proxy sip-server rollover

Use the **sip proxy sip-server rollover** command to configure the rollover behavior of the Session Initiation Protocol (SIP) proxy. This setting specifies the conditions necessary to trigger the proxy to roll over to the next SIP server. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip proxy sip-server rollover service-unavailable-or-timeout
sip proxy sip-server rollover timeout-only

Syntax Description

service-unavailable-or-timeout	Specifies the rollover to the next SIP server to occur after receiving a 503 Service Unavailable message or no response.
timeout-only	Specifies the rollover to the next SIP server to occur only after no response is received.

Default Values

By default, the **sip-server rollover** is set to **timeout-only**.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example sets the SIP server rollover to **service-unavailable-or-timeout**:

(config)**#sip proxy sip-server rollover service-unavailable-or-timeout**

sip proxy sip-server secondary

Use the **sip proxy sip-server secondary** command to configure the secondary Session Initiation Protocol (SIP) softswitch. This command can be entered multiple times to specify numerous secondary softswitches. Use the **no** form of this command to disable this feature. Variations of this command include:

sip proxy sip-server secondary *<hostname | ip address>*
sip proxy sip-server secondary *<hostname | ip address>* **tcp**
sip proxy sip-server secondary *<hostname | ip address>* **tcp** *<port>*
sip proxy sip-server secondary *<hostname | ip address>* **tls** *<profile name>*
sip proxy sip-server secondary *<hostname | ip address>* **tls** *<profile name> <TLS port>*
sip proxy sip-server secondary *<hostname | ip address>* **tls** *<profile name> <TLS port>* **srv** *<service-name-prefix>*
sip proxy sip-server secondary *<hostname | ip address>* **tls** *<profile name> <TLS port>* **srv** *<service-name-prefix> <transport-name-prefix>*
sip proxy sip-server secondary *<hostname | ip address>* **tls** *<profile name>* **srv** *<service-name-prefix>*
sip proxy sip-server secondary *<hostname | ip address>* **tls** *<profile name>* **srv** *<service-name-prefix> <transport-name-prefix>*
sip proxy sip-server secondary *<hostname | ip address>* **udp**
sip proxy sip-server secondary *<hostname | ip address>* **udp** *<port>*

Syntax Description

<hostname | ip address>	Specifies the fully qualified domain name (FQDN) or IP address of the outbound SIP proxy server. IPv4 addresses should be expressed in dotted decimal notation (for example, **208.61.209.2**). IPv6 addresses should be expressed in colon hexadecimal notation (for example, **2001:DB8:1::1**).
tcp	Optional. Configures the softswitch to use Transmission Control Protocol (TCP).
<port>	Optional. Specifies the TCP port used by the softswitch. Range is **1** to **65535**.
tls *<profile name>*	Optional. Specifies the SIP traffic uses Transport Layer Security (TLS). If TLS is specified, a TLS profile must be specified. The TLS profile must have been created prior to issuing this command (refer to the command *tls-profile <profile name> on page 1885*).
<TLS port>	Optional. Specifies the TLS destination port. Range is **1** to **65535**.
srv *<service name prefix>*	Optional. Specifies the service name prefix for the DNS SRV request. Underscores are added automatically.
<transport-name-prefix>	Optional. Specifies the transport prefix for the DNS SRV request. Underscores are added automatically.
udp	Optional. Configures the softswitch to use User Datagram Protocol (UDP).
<port>	Optional. Specifies the UDP port used by the softswitch. Range is **1** to **65535**.

Default Values

By default, no softswitches are configured. If a softswitch is configured, the default protocol is UDP on port **5060**. If a particular protocol is configured and no port is specified, the default port is set to **5060**.

If TLS is used, port **5061** is used by default. By default, SIP TLS requests use **sips** as the service name prefix and **tcp** as the transport name prefix.

Command History

Release 16.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.
Release R13.1.0	Command was expanded to include the **tls** <*profile name*>, <*TLS port*>, and **srv** parameters.

Functional Notes

The guidelines for configuring the softswitch(es) depend on the mode of operation selected. Softswitch configuration is always needed for Stateful mode. It is only needed for Outbound mode and Transparent mode when the SIP Request does not contain any fields that can be resolved to the softswitch's location.

When disabling softswitches, all secondary softswitches must be removed before the primary softswitch can be removed.

If a host name is used to specify the outbound SIP proxy server, a domain naming system (DNS) server must be configured on the AOS unit using the command *name-server on page 1622* or learned via a dynamic IP interface.

To configure the secondary softswitch with a TLS profile, the TLS profile must have been created prior to issuing this command (refer to the command *tls-profile <profile name> on page 1885*). If a specified TLS profile is ever deleted, this softswitch is automatically removed from the AOS device's configuration. If the TLS profile specified by the secondary softswitch is removed from the AOS device configuration, the secondary softswitch is automatically removed from the AOS device configuration.

Usage Examples

The following example sets the secondary softswitch:

(config)**#sip proxy sip-server secondary 208.61.209.2**

sip proxy srtp server *<profile name>*

Use the **sip proxy srtp server** command to configure Secure Realtime Transport Protocol (SRTP) on the on the server side of the Session Initiation Protocol (SIP) proxy. Use the **no** form of this command to disable the SRTP feature. Variations of this command include:

sip proxy srtp server *<profile name>*
sip proxy srtp server *<profile name>* **allow-non-rtp-media**
sip proxy srtp server *<profile name>* **allow-non-rtp-media tls-optional**
sip proxy srtp server *<profile name >* **tls-optional**

Syntax Description

<profile name>	Specifies the SRTP profile name.
allow-non-rtp-media	Optional. Configures the SRTP to allow non-Realtime Transport Protocol (RTP) media, such as T.38 over UDPTL, that cannot be protected by SRTP. When this option is specified, RTP media is secured by SRTP, but any non-RTP media is forwarded unsecured.
tls-optional	Optional. Removes the requirement that SRTP key negotiation is protected by Transport Layer Security (TLS). Adtran does not recommend this configuration.

Default Values

By default, no SRTP profile is configured. If an SRTP profile is configured, it rejects any non-RTP media by default. In addition, if an SRTP profile is configured TLS is required by default.

Functional Notes

SRTP must be configured with a profile name; however, the optional **allow-non-rtp-media** and **tls-optional** parameters can be entered in the CLI in any order, or before the profile name is specified.

Command History

Release R13.3.0	Command was introduced.

Usage Examples

The following example configures an SRTP profile **PROFILE1** on the SIP proxy server that allows non-RTP media:

(config)**#sip proxy srtp server PROFILE1 allow-non-rtp-media**

sip proxy transparent

Use the **sip proxy transparent** command to enable Session Initiation Protocol (SIP) proxy operation in the transparent mode. Use the **no** form of this command to disable this feature. Variations of this command include:

sip proxy transparent
sip proxy transparent nat-simulate
sip proxy transparent ip-spoofing

Syntax Description

nat-simulate	Optional. Specifies the network address translation (NAT) simulation.
ip-spoofing	Optional. Specifies that the source IP address on SIP packets heading towards the phone is replaced with the softswitch IP address.

Default Values

By default, this feature is disabled.

Command History

Release 16.1	Command was introduced.
Release A1	Command was expanded to include the NAT simulation.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.
Release R11.9.0	Command was expanded to include the **ip-spoofing** parameter.

Functional Notes

For an AOS product to use SIP proxy in transparent mode, SIP proxy must be enabled. To enable SIP proxy, enter the **sip proxy** command before entering the **sip proxy transparent** command.

For an AOS data product to use SIP proxy in transparent mode, the firewall SIP application layer gateway (ALG) must be disabled. For more information on disabling the firewall SIP ALG, refer to the command *ip firewall alg on page 1373*.

For more information on the operation and configuration of SIP proxy in transparent mode, refer to the *Configuring SIP Proxy in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables SIP proxy to operate in transparent mode on an AOS voice product:

(config)**#sip proxy**
(config)**#sip proxy transparent**

The following example enables SIP proxy to operate in transparent mode on an AOS data product:

(config)**#no ip firewall alg sip**
(config)**#sip proxy**

(config)**#sip proxy transparent**

sip proxy user-template *<name>*

Use the **sip proxy user-template** command to create a Session Initiation Protocol (SIP) proxy user template and enter the proxy user template configuration mode. Use the **no** form of this command to remove the template. Refer to the *Proxy User Template Command Set on page 4856* for more information.

Syntax Description

<name>	Specifies the name of the proxy user template being created.

Default Values

By default, this feature is disabled.

Command History

Release A4.01	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

Additional information is available in the following sections of this guide:

For more information about SIP proxy, refer to the command *sip proxy on page 1728*. For more information about transparent proxy, refer to the command *sip proxy transparent on page 1764*.

For more information about SIP proxy, refer to the configuration guide *Configuring SIP Proxy in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a proxy user template named **Set1** and enters the proxy user template configuration mode:

```
(config)#sip proxy user-template Set1
(config-template-Set1)#
```

sip qos dscp *<value>*

Use the **sip qos dscp** command to configure the differentiated services code point (DSCP) value to mark Session Initiation Protocol (SIP) packets with. This marking can then be used by the quality of service (QoS) mechanisms to give priority for this type of traffic in the unit. Use the **no** form of this command to disable this feature.

Syntax Description

<value>	Specifies the DSCP value. Valid range is **0** to **63**.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example sets the DSCP value to **63**:

(config)**#sip qos dscp 63**

sip registrar

Use the **sip registrar** command to configure the Session Initiation Protocol (SIP) registrar server used for registering user agents (UAs) into the location database. For more details on SIP operation, refer to the *Technology Review* section of the command *ip firewall alg on page 1373*. Use the **no** form of the **sip registrar** command to disable the registrar server. Variations of this command include:

sip registrar
sip registrar authenticate
sip registrar default-expires <*value*>
sip registrar max-expires <*value*>
sip registrar min-expires <*value*>
sip registrar realm <*string*>

Syntax Description

authenticate	Specifies that authentication is required for each UA during registration.
default-expires <*value*>	Specifies the default expiration period for the UA listing in the location database. UAs requesting registration without specifying an expiration period are given this default expiration period. Range is **0** to **2592000** seconds.
max-expires <*value*>	Specifies the maximum expiration period for the UA listing in the location database. All UAs registering with the SIP proxy server request an expiration period for the listing in the database. UAs requesting an expiration period between the **max-expires** and **min-expires** values are honored. Range is **0** to **2592000** seconds.
min-expires <*value*>	Specifies the minimum expiration period for the UA listing in the location database. All UAs registering with the SIP proxy server request an expiration period for the listing in the database. UAs requesting an expiration period between the **max-expires** and **min-expires** values are honored. Range is **0** to **2592000** seconds.
realm <*string*>	Specifies a realm (using an ASCII character string) for the UA listing in the location database.

Default Values

By default, the registrar server is disabled.

Command History

Release 11.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example sets the default expiration to **5** seconds:

(config)**#sip registrar default-expires 5**

The following example sets the realm string:

(config)**#sip registrar realm voice.adtran.com**

sip secure remote-user

Use the **sip secure remote-user** command to enter the remote user security command set and configure the blacklist options. Use the **no** form of this command to return to the default settings.

Additional subcommands are available once you have entered the SIP Secure Remote User Configuration mode:

blacklist
blacklist attack-threshold <*number*>
blacklist time <*seconds*>

Syntax Description

blacklist	Enables the blacklist to record unauthorized attempts to access the system by an unknown voice user.
attack-threshold <*number*>	Optional. Specifies the number of unauthorized attempts allowed before placing the IPv4 address on the blacklist. Valid range is **1** to **1000**.
time <*seconds*>	Optional. Specifies the number of seconds entries remain on the blacklist before they are automatically removed. Entries do not persist across reboots. Valid range is **0** to **2147483646**. If the time is set to **0**, the entries will be permanent.

Default Values

By default, the **blacklist attack-threshold** is **5** attempts. The **blacklist time** is **3600** seconds.

Functional Notes

When the blacklist is enabled, the system monitors the configured secure ports (refer to *sip udp <port> secure remote-user on page 1783*) for received REGISTER and INVITE attempts from remote voice users that fail to authenticate. SIP server authentication (refer to) and SIP register authentication (refer to) must be enabled to take advantage of the blacklist feature.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example enters the SIP Security Remote User Configuration mode to enable the blacklist and set the attack threshold to **10** and the time to **4800** seconds:

(config)**#sip secure remote-user**
(config-secure-remote)**#blacklist**
(config-secure-remote)**#blacklist attack-threshold 10**
(config-secure-remote)**#blacklist time 4800**

sip session-timer

Use the **sip session-timer** command to configure the Session Initiation Protocol (SIP) session timer. This feature requires user agents (UAs) to periodically send re-INVITE requests (referred to as session refresh requests) to keep the session alive. Use the **no** form of this command to disable the SIP session timer. Variations of this command include:

sip session-timer
sip session timer min-se <*value*>
sip session timer session-expires <*value*>

Syntax Description

min-se <*value*>	Specifies the minimum session interval the unit will accept. The value of this parameter cannot be greater than the value of the **session-expires** parameter. Range is **90** to **3600** seconds.
session-expires <*value*>	Specifies the maximum amount of time that can occur between refresh requests before the session is considered timed out and is torn down. Range is **90** to **3600** seconds.

Default Values

By default, the SIP session timer is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

Entering **sip session-timer** without designating values for **session-expires** or **min-se** assigns the default values **1800** and **90** to **session-expires** and **min-se**, respectively.

Disabling the SIP session timer does not delete the stored values for **min-se** and **session-expires**; it only disables the SIP session timer.

Usage Examples

The following example enables the SIP session timer and sets the session expiration to **2600** seconds:

(config)**#sip session-timer session-expires 2600**

sip timer

Use the **sip timer** command to configure the Session Initiation Protocol (SIP) timers. These timers affect how long a SIP transaction resource is reserved once the final message in a transaction is received. Use the **no** form of this command to return to the default value. Variations of this command include:

sip timer d <*value*>
sip timer d t1-derived
sip timer j <*value*>
sip timer j t1-derived
sip timer T1 <*value*>
sip timer T2 <*value*>

Adtran does not recommend changing T1 and T2 timer values. T1 and T2 timers are base timers within the unit, and any changes will affect other timers which are based off of these timers.

Syntax Description

d <*value*>	Specifies the D timer. Valid range is **0** to **3200** ms.
j <*value*>	Specifies the J timer. Valid range is **0** to **3200** ms.
t1-derived	Specifies that the D or J timer is derived from the T1 timer value. This value is equal to 64*T1 value.
T1 <*value*>	Specifies the T1 timer. This timer is an estimate of network round trip time, and is used as the initial request retransmit interval. Several other SIP timers are derived from the T1 value. Valid range is **50** to **1000** ms.
T2 <*value*>	Specifies the T2 timer. This timer is the maximum retransmit interval for nonINVITE requests and INVITE responses. Valid range is **1000** to **32000** ms.

Default Values

By default, the T1 timer is set to **500** milliseconds, and the T2 timer is set to **4000** milliseconds.

By default, the D and J timers are set to **t1-derived**.

Command History

Release 13.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.
Release R10.10.0	Command was expanded to include the **d** and **j** timers. These parameters replace the **sip transaction fast-terminate** command.

Functional Notes

The D and J timers depend on the T1 timer value for operation. If a value is specified for the D or J timers, the dependence upon the T1 timer value is removed. When the D and J values are configured, timer updates are immediately recognized by the SIP stack. When the D and J timers depend on the T1 timer, they are updated when the T1 value changes.

Usage Examples

The following example configures the T1 timer to **1000** milliseconds:

(config)**#sip timer T1 1000**

sip timer registration-failure-retry *<value>*

Use the **sip timer registration-failure-retry** command to configure the time (in seconds) that will elapse before a Session Initiation Protocol (SIP) endpoint will retry registration with the SIP server after a registration failure has occurred. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies time in seconds. Range is **10** to **604800** seconds.

Default Values

By default, the registration-failure-retry timer is set to **60** seconds.

Command History

Release 11.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example allows a retry attempt to begin after **32** seconds:

(config)**#sip timer registration-failure-retry 32**

sip timer rollover *<value>*

Use the **sip timer rollover** command to specify the time period (in seconds) that the Session Initiation Protocol (SIP) proxy is set to wait for a response to a request before attempting to find an alternate destination. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the time period in seconds. Range is **1** to **32** seconds.

Default Values

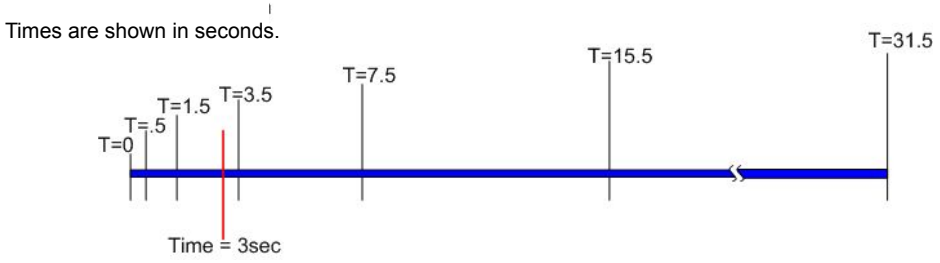
By default, the rollover timer is set to **3** seconds.

Command History

Release 11.1	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

The **sip timer rollover** command sets the SIP timer B value for Invite transactions originating from a SIP trunk. When originating a call, the SIP trunk attempts to send Invite messages to the primary SIP server and waits for a response. If there is no response, the SIP trunk waits for 0.5 seconds before attempting to send another Invite to the same SIP server. If no response, the SIP trunk waits for 1 second before attempting to send another Invite, then waits 2 seconds, and so on. These increasing intervals are shown in the diagram below.



The rollover timer allows the user to control how long to wait before trying the next server. In the diagram above, the red line indicates the rollover timer expiration. If there is no response after the timer expires, the SIP trunk will attempt to send Invite messages to the highest priority backup SIP server obtained via DNS service (SRV). The SIP trunk starts over at T=0 with the next server and doesn't send any more messages to the timed out server. As long as the SIP trunk does not receive a response, it will continue this cycle until it has attempted to contact all the SIP servers.

Usage Examples

The following example allows connection attempts to continue for up to **32** seconds before rolling over to another destination:

(config)**#sip timer rollover 32**

sip timer rollover register

Use the **sip timer rollover register** command to specify the time period (in seconds) that the Session Initiation Protocol (SIP) proxy waits for a response to a REGISTER request before attempting to find an alternate destination. Use the **no** form of this command to return to the default value. Variations of this command include:

sip timer rollover register <*value*>
sip timer rollover register follow-primary

Syntax Description

<*value*>	Specifies the rollover time period for REGISTER events in seconds. Range is **1** to **32** seconds.
follow-primary	Links the rollover timer for REGISTER events to the primary rollover timer specified by the **sip timer rollover** command.

Default Values

By default, the rollover timer for REGISTER events is set to **follow-primary**.

Command History

Release 18.2	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example allows REGISTER request attempts to continue without response for up to **32** seconds before rolling over to another destination:

(config)**#sip timer rollover register 32**

sip timer subscription-failure-retry <*value*>

Use the **sip timer subscription-failure-retry** command to specify the time period (in seconds) that will elapse before a subscription request will be resent to the Session Initiation Protocol (SIP) server after a subscription request failure has occurred. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time period in seconds. Range is **10** to **604800** seconds.

Default Values

By default, the subscription failure retry timer is set to **60** seconds

Command History

Release R13.8.0	Command was introduced.

Usage Examples

The following example allows a retry to occur after **32** seconds:

(config)**#sip timer subscription-failure-retry 32**

sip tls

Use the **sip tls** command to enable Transport Layer Security (TLS) on the AOS device. Use the **no** form of this command to disable TLS. Variations of this command include:

sip tls
sip tls *<port>*

Syntax Description

<port>	Optional. Specifies the Transmission Control Protocol (TCP) port on which the Session Initiation Protocol (SIP) stack listens for TLS packets. Valid range is **1** to **65535**.

Default Values

By default, TLS is disabled. When enabled, the port is set to **5061** by default.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

TLS is a cryptographic protocol that provides communication security over the internet. TLS profiles are created and applied to SIP trunks to provide peer authentication through the exchange of symmetric keys and authentication certificates. Refer to the *SIP TLS Profile Command Set on page 4880* for more information about TLS configuration.

Usage Examples

The following example enables TLS on the AOS device:

(config)**#sip tls**

sip tone-file-prefix

Use the **sip tone-file-prefix** command to specify the file location (flash or CompactFlash) and location prefix of the call progress tone files that the unit should use for blind transfers over Session Initiation Protocol (SIP) trunks operating in local transfer mode. Use the **no** form of this command to return to the default value. Variations of this command include:

sip tone-file-prefix cflash *<location prefix>*
sip tone-file-prefix flash *<location prefix>*

Syntax Description

<location prefix>	Specifies the location prefix of the tone files to be used.
cflash	Specifies that the tone files are located in the unit's CompactFlash.
flash	Specifies that the tone files are located in the unit's flash memory.

Default Values

By default, AOS units with voice features that lack a digital signal processor (DSP) provide North American ringback and disconnect tones.

By default, AOS units with a DSP use the DSP to generate ringback tones based on the system country setting. For more information on how to configure the system country, refer to the command *voice system-country <name> on page 1970*.

Command History

Release R10.1.0	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Functional Notes

This command only designates the file location (flash or CompactFlash) and location prefix of call progress tones used during blind transfers over SIP trunks operating in local transfer mode. To fully configure international call progress tones during blind transfers, you must enable the AOS unit's File Transfer Protocol (FTP) server, upload the appropriate .wav files to the unit using an FTP client, and configure the unit to use the uploaded files. For more information on configuring call progress tones for blind transfers over SIP trunks operating in local transfer mode, refer to the *International Configuration Guide* available on Adtran's Support Forum at https://supportcommunity.adtran.com.

Below is a list of the available countries or regions and their corresponding location prefix.

Australia	**Adtran-UK**	Japan	**Adtran-JP**
Belgium	**Adtran-BE**	Luxembourg	**Adtran-DE**
Canada	**Adtran-NA**	Mexico	**Adtran-MX**
China	**Adtran-CN**	Netherlands	**Adtran-ETSI**
Denmark	**Adtran-ETSI**	Norway	**Adtran-ETSI**
Finland	**Adtran-FI**	Spain	**Adtran-ETSI**
France	**Adtran-FR**	Sweden	**Adtran-ETSI**
Germany	**Adtran-DE**	Switzerland	**Adtran-ETSI**
Hong Kong	**Adtran-HK**	UAE	**Adtran-UK**
India	**Adtran-IN**	UK	**Adtran-UK**
Ireland	**Adtran-IE**	USA	**Adtran-NA**
Italy	**Adtran-ETSI**		

Usage Examples

The following example configures the unit to use tone files stored in flash memory that have the Adtran-UK location prefix:

(config)**#sip tone-file-prefix flash Adtran-UK**

sip trunk-auth-name-source

Use the **sip trunk-auth-name-source** command to configure the authentication name source for the Session Initiation Protocol (SIP) trunks. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip trunk-auth-name-source account-id
sip trunk-auth-name-source message

Syntax Description

account-id	Specifies using the corresponding account ID.
message	Specifies using the To or From user when selecting the authentication name and password.

Default Values

By default, the trunk authentication name source is **message**.

Command History

Release A2.03	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example configures the trunk authentication name source to use the account ID:

(config)**#sip trunk-auth-name-source account-id**

sip udp <*port*> secure remote-user

Use the **sip udp secure remote-user** command to enable remote user security on the specified User Datagram Protocol (UDP) port. This allows SIP traffic only from configured remote voice users, causing SIP traffic from unconfigured remote voice users to be dropped. Use the **no** form of this command to return to the default setting.

Syntax Description

<*port*>	Specifies the UDP port used by the gateway. Range is **1** to **65535**.

Default Values

By default, SIP traffic from any remote voice user is permitted through the UDP port, but if this command is entered, only traffic from configured remote voice users is allowed.

Command History

Release R10.7.0	Command was introduced.
Release R10.8.0	Command syntax was changed to remove the **ip** keyword.

Usage Examples

The following example enables remote user security for UDP port **25069**:

(config)**#sip udp 25069 secure remote-user**

snmp agent

Use the **snmp agent** command to enable the Simple Network Management Protocol (SNMP) agent. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the SNMP agent is disabled.

Command History

Release 1.1	Command was introduced.
Release 18.2	Command was changed from **ip snmp agent** to **snmp agent** to incorporate Internet Protocol version 6 (IPv6) for Adtran internetworking products only.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword in Adtran voice products.

Functional Notes

Allows a MIB browser to access standard MIBs within the product. This also allows the product to send traps to a trap management station.

SNMP can be used with either Internet Protocol version 4 (IPv4) or IPv6.

Usage Examples

The following example enables the IP SNMP agent:

(config)**#snmp agent**

snmp ifmib alias long

Use the **snmp ifmib alias long** command to configure the Simple Network Management Protocol (SNMP) IF.MIB alias settings to allow an alias string to be up to 255 characters long. Use the **no** form of this command to return to the default SNMP IF.MIB setting.

Syntax Description

No subcommands.

Default Values

By default, the maximum length of the SNMP IF.MIB alias is **64** characters.

Command History

Release 17.4	Command was introduced.

Usage Examples

The following example enables a longer SNMP IF.MIB alias length:

(config)**#snmp ifmib alias long**

snmp-server chassis-id "<*string*>"

Use the **snmp-server chassis-id** command to specify an identifier for the Simple Network Management Protocol (SNMP) server. Use the **no** form of this command to return to the default value.

Syntax Description

"<string>"	Identifies the product using an alphanumeric string enclosed in quotation marks (up to 32 characters in length).

Default Values

By default, the **snmp-server chassis-id** is set to **Chassis ID**.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example configures a chassis ID of **A432692**:

(config)**#snmp-server chassis-id A432692**

snmp-server community

Use the **snmp-server community** command to specify a community string to control access to the Simple Network Management Protocol (SNMP) information. Use the **no** form of this command to remove a specified community. Variations of this command include:

snmp-server community <*community*>
snmp-server community <*community*> **[ip access-class** <*ipv4 acl*>**] [ipv6 access-class** <*ipv6 acl*>**]**
snmp-server community <*community*> **[ip access-class** <*ipv4 acl*>**] [ipv6 access-class** <*ipv6 acl*>**]** **[any-vrf | vrf** <*name*>**]**
snmp-server community <*community*> **ro**
snmp-server community <*community*> **ro [ip access-class** <*ipv4 acl*>**] [ipv6 access-class** <*ipv6 acl*>**]**
snmp-server community <*community*> **ro [ip access-class** <*ipv4 acl*>**] [ipv6 access-class** <*ipv6 acl*>**]** **[any-vrf | vrf** <*name*>**]**
snmp-server community <*community*> **rw**
snmp-server community <*community*> **rw [ip access-class** <*ipv4 acl*>**] [ipv6 access-class** <*ipv6 acl*>**]**
snmp-server community <*community*> **rw [ip access-class** <*ipv4 acl*>**] [ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server community <*community*> **view** <*name*>
snmp-server community <*community*> **view** <*name*> **[ip access-class** <*ipv4 acl*>**]** **[ipv6 access-class** <*ipv6 acl*>**]**
snmp-server community <*community*> **view** <*name*> **[ip access-class** <*ipv4 acl*>**]** **[ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server community <*community*> **view** <*name*> **ro**
snmp-server community <*community*> **view** <*name*> **ro [ip access-class** <*ipv4 acl*>**]** **[ipv6 access-class** <*ipv6 acl*>**]**
snmp-server community <*community*> **view** <*name*> **ro [ip access-class** <*ipv4 acl*>**]** **[ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server community <*community*> **view** <*name*> **rw**
snmp-server community <*community*> **view** <*name*> **rw [ip access-class** <*ipv4 acl*>**]** **[ipv6 access-class** <*ipv6 acl*>**]**
snmp-server community <*community*> **view** <*name*> **rw [ip access-class** <*ipv4 acl*>**]** **[ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**

Syntax Description

<*community*>	Specifies the community string (a password to grant SNMP access).
ip access-class <*ipv4 acl*>	Optional. Specifies an Internet Protocol version 4 (IPv4) access control list (ACL) name used to limit access. Refer to *ip access-list extended <ipv4 acl name> on page 1344* and *ip access-list standard <ipv4 acl name> on page 1346* for more information on creating IPv4 ACLs
ipv6 access-class <*ipv6 acl*>	Optional. Specifies an Internet Protocol version 6 (IPv6) ACL name used to limit access. Refer to *ipv6 access-list extended <ipv6 acl name> on page 1500* and *ipv6 access-list standard <ipv6 acl name> on page 1502* for more information on creating IPv6 ACLs.
ro	Optional. Grants read-only access, allowing retrieval of MIB objects.

rw	Optional. Grants read-write access, allowing retrieval and modification of MIB objects.
view <*name*>	Optional. Specifies a previously defined view. Views define specific MIB objects available to the specified community string. For information on creating a new view, refer to *snmp-server view <name> <value> on page 1831*.
any-vrf	Optional. Specifies the ACL is applied to any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Specifies the ACL is applied to a specific VRF instance.

*The parameters [**any-vrf** | **vrf** <name>] can only be entered if an **ip access-class** or **ipv6 access-class** is specified.*

Default Values

By default, there are no configured SNMP communities.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include the **view** parameter.
Release 18.2	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran internetworking products only.
Release R10.1.0	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran voice products.
Release R10.8.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

SNMP server communities can specify up to two ACLs to control access, one each for IPv4 and IPv6 protocols. When two ACLs are used, they must use the same VRF restriction (the default VRF, any VRF, or a specific VRF.) If no VRF is named, the default unnamed VRF is assumed.

Usage Examples

The following example specifies a community named **MyCommunity**, specifies a previously defined view named **blockinterfaces**, and assigns read-write access:

(config)**#snmp-server community MyCommunity view blockinterfaces rw**

snmp-server contact

Use the **snmp-server contact** command to specify Simple Network Management Protocol (SNMP) server contact information. Use the **no** form of this command to remove a configured contact. Variations of this command include:

snmp-server contact email <*address*>
snmp-server contact pager <*number*>
snmp-server contact phone <*number*>
snmp-server contact *"<string>"*

Syntax Description

email <*address*>	Specifies email address for the SNMP server contact.
pager <*number*>	Specifies pager number for the SNMP server contact.
phone <*number*>	Specifies phone number for the SNMP server contact.
"<string>"	Populates the sysContact string using an alphanumeric string enclosed in quotation marks (up to 32 characters in length).

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example specifies **6536999** for the pager number:

(config)**#snmp-server contact pager 6536999**

snmp-server context <*string*> vrf <*name*>

Use the **snmp-server context vrf** command to map the Simple Network Management Protocol (SNMP) context to the appropriate non-default virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

context <*string*>	Specifies the SNMP context name.
vrf <*ame*>	Specifies the non-default VRF instance to which to map the SNMP context.

Default Values

By default, there are no VRF context mappings.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

VRF context mapping is used to map the context of SNMP requests to the appropriate VRF instance. This is only necessary in multi-VRF installations where the content of the following four management information base (MIB) tables are used:

- IP-MIB::ipAddressTable
- IP-MIB::ipAddrTable
- IP-FORWARD-MIB::inetCidrRouteTable
- IP-FORWARD-MIB::ipCidrRouteTable

Context mapping does not apply to SNMP version 1 and version 2.

If your installation meets the above requirements, additional steps must be taken to ensure SNMP requests reach the correct destination.

- Define VRF instances on the AOS router. (Refer to *Configuring Multi-VRF in AOS* for more information.)
- Define a VRF context mapping to associate the VRF instance to the appropriate context name.
- Create an SNMP group for each non-default VRF instance. (Refer to the command *snmp-server group on page 1799* for more information.)
- Create an SNMP user and associate the user to appropriate SNMP group for each VRF instance. (Refer to *snmp-server user on page 1821* command for more information.)

Usage Examples

The following example maps the SNMP context **RED-CONTEXT** to the VRF instance **RED**:

(config)**#snmp-server context RED-CONTEXT vrf RED**

snmp-server enable traps

Use the **snmp-server enable traps** command to enable all Simple Network Management Protocol (SNMP) traps available on your system. Use the **no** form of this command to disable SNMP traps. Variations of this command include:

snmp-server enable traps
snmp-server enable traps application
snmp-server enable traps battery
snmp-server enable traps bgp
snmp-server enable traps delay track <*name*>
snmp-server enable traps dying-gasp
snmp-server enable traps entity
snmp-server enable traps eps
snmp-server enable traps fan
snmp-server enable traps frame-relay
snmp-server enable traps network-sync
snmp-server enable traps resource
snmp-server enable traps rps
snmp-server enable traps sfp
snmp-server enable traps snmp
snmp-server enable traps unit
snmp-server enable traps track
snmp-server enable traps voice
snmp-server enable traps vrrp

Syntax Description

application	Optional. Enables SNMP traps for applications (such as, Domain Naming System (DNS) traps).
battery	Optional. Enables traps for battery status.
bgp	Optional. Enables the Border Gateway Protocol (BGP) traps.
dying-gasp	Optional. Enables the dying-gasp traps. Refer to the **Functional Notes** below for more information on configuring a dying-gasp trap host.
delay track <*name*>	Optional. Enables SNMP traps to be buffered instead of sent immediately based on the status of the named track.
entity	Optional. Enables the entity sensor traps such as insertion and deletion of a small form-factor pluggable (SFP) interface module.
eps	Optional. Enables the external power supply (EPS) traps for connection state changes and failures.
fan	Optional. Enables the fan failure notification traps.
frame-relay	Optional. Enables the Frame Relay notification traps.
network-sync	Optional. Enables the network synchronization notification traps.
resource	Optional. Enables the resource utilization notification traps. This option is only available on AOS voice products.

rps	Optional. Enables the redundant power supply (RPS) traps for connection state changes and failures.
sfp	Optional. Enables the small form-factor pluggable (SFP) traps.
snmp	Optional. Enables the SNMP notification traps. The following SNMP traps are supported: **coldStart** **warmStart** **linkUp** **linkDown** **authenticationFailure**
track	Optional. Enables the network monitor track traps.
unit	Optional. Enables user login/logout traps for the unit.
voice	Optional. Enables voice notification traps.
vrrp	Optional. Enables Virtual Router Redundancy Protocol version 2 (VRRPv2) and version 3 (VRRPv3) traps.

Default Values

By default, there are no traps enabled.

Command History

Release 1.1	Command was introduced.
Release 17.3	Command was expanded to include the Frame Relay.
Release 17.6	Command was expanded to include **voice** traps.
Release A2.04	Command was expanded to include **resource** traps.
Release 18.1	Command was expanded to include **bgp** and **track** traps.
Release R10.3.0	Command was expanded to include **application** traps.
Release R10.8.0	Command was expanded to include **eps** and **rps** traps.
Release R10.11.0	Command was expanded to include **entity**, **fan** and **network-sync** traps.
Release R11.3.0	Command was expanded to include **vrrp** traps.
Release R11.6.0	Command was expanded to include **dying-gasp** traps.
Release R11.11.0	Command was expanded to include **battery** traps.
Release R13.3.0	Command was expanded to include **sfp** and **unit** traps. Added the ability to delay traps for tracks.

Functional Notes

Resource utilization traps are configured by using the command *resource-utilization on page 1684*.

If **dying-gasp** traps are enabled, the SNMP host must be configured separately to receive the traps using the **snmp-server host** [*<ip address>* | **vrf** *<name> <ip address>*] **dying-gasp-traps [1 | 2]** command. Refer to *snmp-server host dying-gasp-traps on page 1807* for more information.

Usage Examples

The following example enables SNMP traps:

(config)**#snmp-server enable traps snmp**

The following example enables all traps:

(config)**#snmp-server enable traps**

snmp-server engineID local <*hex string*>

Use the **snmp-server engineID local** command to change the default and manually set the Simple Network Management Protocol (SNMP) version 3 (v3) engine ID for the local machine. Use the **no** form of this command to return to the default engine ID.

Syntax Description

<hex string>	Defines the engine ID for the system. Engine IDs are the 12-octet hexadecimal representation (24 characters using 0 through 9 and/or a through f) defining a system on the management domain. Refer to the *Technology Review* for more detailed information on engine ID octet assignments.

SNMP v3 requires unique engine IDs for all systems in the management domain. Use the default engine ID when possible to ensure the uniqueness of the numbers. Problems can occur on a management network that contains duplicate engine IDs.

Default Values

By default, the local SNMP-server engine ID is **8000029803xxxxxxxxxxxx** (where the string of Xs represents the system medium access control (MAC) address).

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example changes the default engine ID for the local system to **80 00 02 98 00 00 00 00 00 00 01** (where **80 00 02 98** represents the Internet Assigned Numbers Authority (IANA) ID for Adtran and **00 00 00 00 00 00 01** arbitrarily represents the first system on the management domain):

(config)**#snmp-server engineID local 800002980000000000000001**

Technology Review

The SNMP v3 engine ID is a unique identifier for a system on a management domain. The default engine ID contains 11 octets (in hexadecimal notation) that represent certain information about the system. The default engine ID format is as follows:

Octets 1 to 4	Octet 5	Octets 6 to 11
IANA ID for the product manufacturer	**03** Identifies that octets 6 through 11 contain a MAC address	System MAC address

The first 4 octets of the default engine ID for Adtran products is 80000298. Octets 1 through 4 represent the SNMP private enterprise number (assigned by the IANA) for the product manufacturer. The leading bit of octet 1 (the most significant bit) will always be a 1 for a default engine ID (making the leading character in the hex string an 8). Adtran products use the IANA ID of 664 (which is 02 98 in hexadecimal notation). Octet 5 is set to 03 to indicate that the engine ID uses a MAC address as the unique identifier. The last six octets of the default engine ID for Adtran routers contain the MAC address for the Ethernet 0/1 interface (for example, 00127905257c).

The **snmp-server engineID local** command overrides the default engine ID and replaces it with the first 24 characters of the user-entered string. Because the string is in hexadecimal notation, only numbers 0 through 9 and characters a through f are valid. If fewer than 24 characters are entered in the string, pad the end of the entered string with zeros (least significant bits) until the 24-character string is complete. For example, a user input of 8000029805 results in an engine ID of 800002980500000000000000.

snmp-server engineID remote

Use the **snmp-server engineID remote** command to identify a remote Simple Network Management Protocol (SNMP) entity's engine ID. The remote engine ID is necessary before SNMP version 3 (SNMPv3) inform notifications can be acknowledged. Refer to the command *snmp-server user on page 1821* for additional information about how it is used in conjunction with this command. Use the **no** form of this command to remove the remote SNMP entity's engine ID. Variations of this command include:

snmp-server engineID remote auto-link *<hex string>*
snmp-server engineID remote *<ip address> <hex string>*
snmp-server engineID remote vrf *<name> <ip address> <hex string>*

Syntax Description

auto-link	Specifies that the remote SNMP device Internet Protocol version 4 (IPv4) address follows the active auto-link server.
<ip address>	Specifies the IPv4 or Internet Protocol version 6 (IPv6) address for the remote SNMP device. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal format X:X:X:X::X, for example, **2001:DB8:1::1**.
<hex string>	Specifies the engine ID for the remote SNMP device.
vrf <name>	Specifies the VRF instance on which the remote SNMP device exists. If no VRF is specified, the SNMP device exists on the default unnamed VRF.

Default Values

By default, there are no remote engine IDs identified.

Command History

Release 14.1	Command was introduced.
Release R10.7.0	Command was expanded to include the **auto-link** parameter.
Release R10.8.0	Command was expanded to include the **vrf** *<name>* parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Use the following requirements to avoid errors when configuring SNMP server and multi-VRF in AOS:

- For a remote engine ID with a VRF specified, a remote user with the same host address and VRF must be configured.
- If a VRF name is not specified for the remote engine ID and user, the default VRF will be used.
- A VRF associated with a remote address must be the same as the access class list (ACL) VRF and must match the remote engineID VRF. If they do not match, an error will display.

Usage Examples

The following example identifies a remote SNMP device with an IPv4 address of **10.10.12.2** and an engine ID of **80000298000000A0C8000001**:

(config)**#snmp-server engineID remote 10.10.12.2 80000298000000A0C8000001**

snmp-server group

Use the **snmp-server group** command to specify a new Simple Network Management Protocol (SNMP) server group to control access to SNMP information. Use the **no** form of this command to remove a specified group. Variations of this command include:

snmp-server group <*groupname*> **v1**
snmp-server group <*groupname*> **v1 [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**]**
[notify <*name*>**] [read** <*name*>**] [write** <*name*>**] [any-vrf | vrf** <*name*>**]**
snmp-server group <*groupname*> **v2c**
snmp-server group <*groupname*> **v2c [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**]**
[notify <*name*>**] [read** <*name*>**] [write** <*name*>**] [any-vrf | vrf** <*name*>**]**
snmp-server group <*groupname*> **v3 auth**
snmp-server group <*groupname*> **v3 auth context** <*string*>
snmp-server group <*groupname*> **v3 auth [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**]**
[notify <*name*>**] [read** <*name*>**] [write** <*name*>**] [any-vrf | vrf** <*name*>**]**
snmp-server group <*groupname*> **v3 auth context** <*string*> **[ip access-class** <*ipv4 acl*> **| ipv6**
access-class <*ipv6 acl*>**] [notify** <*name*>**] [read** <*name*>**] [write** <*name*>**] [any-vrf | vrf** <*name*>**]**
snmp-server group <*groupname*> **v3 noauth**
snmp-server group <*groupname*> **v3 noauth context** <*string*>
snmp-server group <*groupname*> **v3 noauth [ip access-class** <*ipv4 acl*> **| ipv6 access-class**
<*ipv6 acl*>**] [notify** <*name*> | **read** <*name*> | **write** <*name*>**] [any-vrf | vrf** <*name*>**]**
snmp-server group <*groupname*> **v3 noauth context** <*string*> **[ip access-class** <*ipv4 acl*> **| ipv6**
access-class <*ipv6 acl*>**] [notify** <*name*> | **read** <*name*> | **write** <*name*>**] [any-vrf |**
vrf <*name*>**]**
snmp-server group <*groupname*> **v3 priv**
snmp-server group <*groupname*> **v3 priv context** <*string*>
snmp-server group <*groupname*> **v3 priv [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**]**
[notify <*name*>**] [read** <*name*>**] [write** <*name*>**] [any-vrf | vrf** <*name*>**]**
snmp-server group <*groupname*> **v3 priv context** <*string*> **[ip access-class** <*ipv4 acl*> **| ipv6**
access-class <*ipv6 acl*>**] [notify** <*name*>**] [read** <*name*>**] [write** <*name*>**] [any-vrf | vrf** <*name*>**]**

Syntax Description

<*groupname*>	Specifies the name of the SNMP server group (32 characters maximum).
v1	Specifies using SNMP version 1 security model.
v2c	Specifies using SNMP version 2c security model.
v3	Specifies using SNMP version 3 user-based security model (USM).
auth	Optional. Only used in SNMP version 3. Indicates that authentication is used.
noauth	Optional. Only used in SNMP version 3. Indicates that no authentication is used.
priv	Optional. Only used in SNMP version 3. Indicates that privacy authentication is used.

context <*string*>	Optional. Only used in SNMP version 3 with multi-VRF installations. Specifies a context for VRF context mapping.
ip access-class <*ipv4 acl*>	Optional. Specifies an Internet Protocol version 4 (IPv4) access control list (ACL) entry.
ipv6 access-class <*ipv6 acl*>	Optional. Specifies an Internet Protocol version 6 (IPv6) ACL entry.
notify <*name*>	Optional. Specifies a previously configured SNMP view name to which the group has notify access (32 characters maximum). If a view is not specified, the system automatically assigned a default notify-view with no restrictions.
read <*name*>	Optional. Specifies a previously configured SNMP view name to which the group has read access (32 characters maximum). If a view is not specified, the system automatically assigned a default read-view with no restrictions.
write <*name*>	Optional. Specifies a previously configured SNMP view name to which the group has write access(32 characters maximum). If a write-view is not specified, write access is restricted for all users of the group.
any-vrf	Optional. Specifies the ACL is applied to any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Specifies the ACL is applied to a specific non-default VRF instance.

Default Values

If no views are specified, the system automatically assigns default read- and notify-views that have no restrictions.

Command History

Release 13.1	Command was introduced.
Release 18.2	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran internetworking products only.
Release R10.1.0	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran voice products.
Release R10.8.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.
Release R10.11.0	Command was expanded to include the **context** <*string*> parameter.

Functional Notes

SNMP groups are used to map SNMP users to SNMP views. To create a group, specify one or more views to which users will have access. A given view can be accessed by more than one group, as needed.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

SNMP context mapping is only used in conjunction with multi-VRF configurations to ensure proper delivery of SNMP requests. The SNMP context is mapped to a specific VRF instance to differentiate between the same IP address used across multiple VRFs.

SNMP server communities can specify up to two ACLs to control access, one each for IPv4 and IPv6 protocols. When two ACLs are used, they must use the same VRF restriction (the default VRF, any VRF, or a specific VRF.) If no VRF is named, the default unnamed VRF is assumed.

Usage Examples

The following example defines a group called **securityV3auth** using version 3 security model, authentication, and no ACL to verify:

(config)**#snmp-server group securityV3auth v3 auth**

snmp-server host auto-link dying-gasp-traps

Use the **snmp-server host auto-link dying-gasp-traps** command to configure the unit to send Simple Network Management Protocol (SNMP) dying-gasp traps messages to the active auto-link server. Use the **no** form of this command to disable the setting. Variations of this command include the following:

snmp-server host auto-link dying-gasp-traps 1 <*community*>
snmp-server host auto-linkdying-gasp-traps 1 version 1 <*community*>
snmp-server host auto-link dying-gasp-traps 1 version 2c <*community*>
snmp-server host auto-link dying-gasp-traps 1 version 3 auth <*user name*>
snmp-server host auto-link dying-gasp-traps 1 version 3 noauth <*user name*>
snmp-server host auto-link dying-gasp-traps 1 version 3 priv <*user name*>
snmp-server host auto-link dying-gasp-traps 2 <*community*>
snmp-server host auto-link dying-gasp-traps 2 version 1 <*community*>
snmp-server host auto-link dying-gasp-traps 2 version 2c <*community*>
snmp-server host auto-link dying-gasp-traps 2 version 3 auth <*user name*>
snmp-server host auto-link dying-gasp-traps 2 version 3 noauth <*user name*>
snmp-server host auto-link dying-gasp-traps 2 version 3 priv <*user name*>

Syntax Description

version 1	Specifies using SNMP version 1 security model.
version 2c	Specifies using SNMP version 2c security model.
version 3	Specifies using SNMP version 3 user-based security model (USM).
auth	Only used in SNMP version 3. Indicates that authentication is used.
noauth	Only used in SNMP version 3. Indicates that no authentication is used.
priv	Only used in SNMP version 3. Indicates that privacy authentication is used.
<*community*>	Specifies the community string (used as a password, 16 characters maximum) for authorized agents to obtain access to SNMP information.
<*user name*>	Specifies the user name for SNMP version 3 security.

Default Values

No default values are necessary for this command.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example configures an auto-link host as the first priority server to receive dying-gasp traps using SNMP **version 2c** and sets the community string to **MyCommunity**:

(config)**#snmp-server host auto-link dying-gasp-traps 1 version 2c MyCommunity**

snmp-server host auto-link informs

Use the **snmp-server host auto-link informs** command to configure the unit to send Simple Network Management Protocol (SNMP) INFORM messages to the active auto-link server. Use the **no** form of this command to disable the setting. Variations of this command include the following:

snmp-server host auto-link informs <*community*>
snmp-server host auto-link informs version 1 <*community*>
snmp-server host auto-link informs version 1 <*community*> **battery**
snmp-server host auto-link informs version 1 <*community*> **eps**
snmp-server host auto-link informs version 1 <*community*> **rps**
snmp-server host auto-link informs version 1 <*community*> **sfp**
snmp-server host auto-link informs version 1 <*community*> **snmp**
snmp-server host auto-link informs version 1 <*community*> **unit**
snmp-server host auto-link informs version 2c <*community*>
snmp-server host auto-link informs version 2c <*community*> **battery**
snmp-server host auto-link informs version 2c <*community*> **eps**
snmp-server host auto-link informs version 2c <*community*> **rps**
snmp-server host auto-link informs version 2c <*community*> **sfp**
snmp-server host auto-link informs version 2c <*community*> **snmp**
snmp-server host auto-link informs version 2c <*community*> **unit**
snmp-server host auto-link informs version 3 auth <*community*>
snmp-server host auto-link informs version 3 auth <*community*> **battery**
snmp-server host auto-link informs version 3 auth <*community*> **eps**
snmp-server host auto-link informs version 3 auth <*community*> **rps**
snmp-server host auto-link informs version 3 auth <*community*> **sfp**
snmp-server host auto-link informs version 3 auth <*community*> **snmp**
snmp-server host auto-link informs version 3 auth <*community*> **unit**
snmp-server host auto-link informs version 3 noauth <*community*>
snmp-server host auto-link informs version 3 noauth <*community*> **battery**
snmp-server host auto-link informs version 3 noauth <*community*> **eps**
snmp-server host auto-link informs version 3 noauth <*community*> **rps**
snmp-server host auto-link informs version 3 noauth <*community*> **sfp**
snmp-server host auto-link informs version 3 noauth <*community*> **snmp**
snmp-server host auto-link informs version 3 noauth <*community*> **unit**
snmp-server host auto-link informs version 3 priv <*community*>
snmp-server host auto-link informs version 3 priv <*community*> **battery**
snmp-server host auto-link informs version 3 priv <*community*> **eps**
snmp-server host auto-link informs version 3 priv <*community*> **rps**
snmp-server host auto-link informs version 3 priv <*community*> **sfp**
snmp-server host auto-link informs version 3 priv <*community*> **snmp**
snmp-server host auto-link informs version 3 priv <*community*> **unit**

Syntax Description

version 1	Specifies using SNMP version 1 security model.
version 2c	Specifies using SNMP version 2c security model.

version 3	Specifies using SNMP version 3 user-based security model (USM).
auth	Only used in SNMP version 3. Indicates that authentication is used.
noauth	Only used in SNMP version 3. Indicates that no authentication is used.
priv	Only used in SNMP version 3. Indicates that privacy authentication is used.
<*community*>	Specifies the community string (used as a password) (16 characters maximum) for authorized agents to obtain access to SNMP information.
battery	Optional. Allows battery trap informs.
eps	Optional. Allows external power supply (EPS) informs.
rps	Optional. Allows redundant power supply (RPS) informs.
sfp	Optional. Allows small form-factor pluggable (SFP) informs.
snmp	Optional. Allows SNMP informs.
unit	Optional. Allows unit informs for user login/logout.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **eps** and **rps** parameters.
Release R11.11.0	Command was expanded to include the **battery** parameter.
Release R13.2.0	Command was expanded to include the **sfp** and **unit** parameters.

Usage Examples

The following example sends all SNMP informs to the auto-link host and community string **MyCommunity** using SNMP **version 2c**:

(config)**#snmp-server host auto-link informs version 2c MyCommunity snmp**

snmp-server host auto-link traps

Use the **snmp-server host auto-link traps** command to configure the unit to send traps to the active auto-link server. Use the **no** form of this command to disable the setting. Variations of this command include the following:

snmp-server host auto-link traps <*community*>
snmp-server host auto-link traps version 1 <*community*> **[application] [battery] [bgp] [entity] [eps] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host auto-link traps version 2c <*community*> **[application] [battery] [bgp] [entity] [eps] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host auto-link traps version 3 auth <*community*> **[application] [battery] [bgp] [entity] [eps] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host auto-link traps version 3 noauth <*community*> **[application] [battery] [bgp] [entity] [eps] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host auto-link traps version 3 priv <*community*> **[application] [battery] [bgp] [entity] [eps] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**

Syntax Description

version 1	Specifies using Simple Network Management Protocol (SNMP) version 1 security model.
version 2c	Specifies using SNMP version 2c security model.
version 3	Specifies using SNMP version 3 user-based security model (USM).
auth	Only used in SNMP version 3. Indicates that authentication is used.
noauth	Only used in SNMP version 3. Indicates that no authentication is used.
priv	Only used in SNMP version 3. Indicates that privacy authentication is used.
<*community*>	Specifies the community string (used as a password) (16 characters maximum) for authorized agents to obtain access to SNMP information.
application	Optional. Allows application traps (such as, Domain Naming System (DNS) traps).
battery	Optional. Enables battery status traps.
bgp	Optional. Allows Border Gateway Protocol (BGP) traps.
entity	Optional. Enables the entity sensor traps such as insertion and deletion of a small form-factor pluggable (SFP) interface module.
eps	Optional. Allows external power supply (EPS) traps.
fan	Optional. Enables the fan failure notification trap.
frame-relay	Optional. Allows Frame Relay traps.
network-sync	Optional. Enables the network synchronization notification traps.
over-temperature	Optional. Enables the over-temperature protection traps.

resource	Optional. Enables the resource utilization set of traps.
rps	Optional. Allows redundant power supply (RPS) traps.
sfp	Optional. Allows small form-factor pluggable (SFP) traps.
snmp	Optional. Allows SNMP traps.
unit	Optional. Allows unit traps for user login/logout.
track	Optional. Allows network monitor track traps.
voice	Optional. Allows voice traps.
vrrp	Optional. Allows Virtual Router Redundancy Protocol version 2 (VRRPv2) and version 3 (VRRPv3) traps.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.6	Command was expanded to include the **frame-relay** parameter.
Release 17.9	Command was expanded to include more **frame-relay** options, more **snmp** options, and the **voice** parameter. In addition, the **snmp-server host** <*ip address*> **traps version 3 priv** <*community*> version of the command was removed.
Release A2.04	Command was expanded to include **resource** traps.
Release 18.1	Command was expanded to include the **bgp** and **track** parameter.
Release R10.4.0	Command was expanded to include the **application** parameter.
Release R10.8.0	Command was expanded to include the **eps** and **rps** parameters.
Release R10.11.0	Command was expanded to include **entity, fan**, and **network-sync** traps.
Release R11.3.0	Command was expanded to include **vrrp** traps.
Release R11.6.0	Command was expanded to include the **over-temperature** protection.
Release R11.11.0	Command was expanded to include **battery** traps.
Release R13.2.0	Command was expanded to include the **sfp** and **unit** parameters.

Usage Examples

The following example sends all enabled traps to the auto-link host using SNMP **version 2c** and sets the community string to **MyCommunity**:

(config)**#snmp-server host auto-link traps version 2c MyCommunity**

snmp-server host dying-gasp-traps

Use the **snmp-server host dying-gasp-traps** command to configure the unit to send Simple Network Management Protocol (SNMP) dying-gasp traps messages to the specified SNMP host. Use the **no** form of this command to remove a specified host. Variations of this command include the following:

snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 1** <*community*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 1 version 1** <*community*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 1 version 2c** <*community*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 1 version 3 auth** <*user name*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 1 version 3 noauth** <*user name*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 1 version 3 priv** <*user name*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 2** <*community*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 2 version 1** <*community*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 2 version 2c** <*community*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 2 version 3 auth** <*user name*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 2 version 3 noauth** <*user name*>
snmp-server host [<*ip address*> | <*name*>**] dying-gasp-traps 2 version 3 priv** <*user name*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 1** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 1 version 1** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 1 version 2c** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 1 version 3 auth** <*user name*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 1 version 3 noauth** <*user name*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 1 version 3 priv** <*user name*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 2** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 2 version 1** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 2 version 2c** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 2 version 3 auth** <*user name*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 2 version 3 noauth** <*user name*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] dying-gasp-traps 2 version 3 priv** <*user name*>

Syntax Description

<*ip address*>	Specifies the IP address (either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6)) of the SNMP host that receives the SNMP information. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal format X:X:X:X::X, for example, **2001:DB8:1::1**.
<name>	Specifies the Fully Qualified Domain Name (FQDN) (e.g., **adtran.com**) of the SNMP host that receives the SNMP information.

vrf <*name*>	Optional. Specifies the VRF instance on which the host exists. If a VRF instance is not specified, the default unnamed VRF is assumed.
version 1	Specifies using SNMP version 1 security model.
version 2c	Specifies using SNMP version 2c security model.
version 3	Specifies using SNMP version 3 user-based security model (USM).
auth	Only used in SNMP version 3. Indicates that authentication is used.
noauth	Only used in SNMP version 3. Indicates that no authentication is used.
priv	Only used in SNMP version 3. Indicates that privacy authentication is used.
<*community*>	Specifies the community string (used as a password, 16 characters maximum) for authorized agents to obtain access to SNMP information.
<*user name*>	Specifies the user name for SNMP version 3 security.

Default Values

No default values are necessary for this command.

Command History

Release R11.6.0	Command was introduced.
Release R13.3.0	Command was expanded to allow the <*name*> of a FQDN server to be specified as the recipient of SNMP information.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example configures an SNMP server host at IPv4 address **190.3.44.69** as the first priority server to receive dying-gasp traps using SNMP **version 2c** and set the community string to **MyCommunity**:

(config)**#snmp-server host 190.3.44.69 dying-gasp-traps 1 version 2c MyCommunity**

snmp-server host informs

Use the **snmp-server host informs** command to configure the unit to send Simple Network Management Protocol (SNMP) INFORM messages to the specified SNMP host. Use the **no** form of this command to remove a specified host. Variations of this command include the following:

snmp-server host [<*ip address*> | <*name*>**] informs** <*community*>
snmp-server host [<*ip address*> | <*name*>**] informs version 1** <*community*>
snmp-server host [<*ip address*> | <*name*>**] informs version 1** <*community*> **[battery] [eps] [rps] [sfp] [snmp] [unit]**
snmp-server host [<*ip address*> | <*name*>**] informs version 2c** <*community*>
snmp-server host [<*ip address*> | <*name*>**] informs version 2c** <*community*> **[battery] [eps] [rps] [sfp] [snmp] [unit]**
snmp-server host [<*ip address*> | <*name*>**] informs version 3 auth** <*community*>
snmp-server host [<*ip address*> | <*name*>**] informs version 3 auth** <*community*> **[battery] [eps] [rps] [sfp] [snmp] [unit]**
snmp-server host [<*ip address*> | <*name*>**] informs version 3 noauth** <*community*>
snmp-server host [<*ip address*> | <*name*>**] informs version 3 noauth** <*community*> **[battery] [eps] [rps] [sfp] [snmp] [unit]**
snmp-server host [<*ip address*> | <*name*>**] informs version 3 priv** <*community*>
snmp-server host [<*ip address*> | <*name*>**] informs version 3 priv** <*community*> **[battery] [eps] [rps] [sfp] [snmp] [unit]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 1** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 1** <*community*> **[battery] [sfp] [snmp] [unit]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 2c** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 2c** <*community*> **[battery] [sfp] [snmp] [unit]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 3 auth** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 3 auth** <*community*> **[battery] [sfp] [snmp] [unit]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 3 noauth** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 3 noauth** <*community*> **[battery] [sfp] [snmp] [unit]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 3 priv** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] informs version 3 priv** <*community*> **[battery] [sfp] [snmp] [unit]**

Syntax Description

<*ip address*>	Specifies the IP address (either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6)) of the SNMP host that receives the SNMP information. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal format X:X:X:X::X, for example, **2001:DB8:1::1**.

<name>	Specifies the Fully Qualified Domain Name (FQDN) (e.g., **adtran.com**) of the SNMP host that receives the SNMP information.
vrf *<name>*	Optional. Specifies the VRF instance on which the host exists. If a VRF instance is not specified, the default unnamed VRF is assumed.
version 1	Specifies using SNMP version 1 security model.
version 2c	Specifies using SNMP version 2c security model.
version 3	Specifies using SNMP version 3 user-based security model (USM).
auth	Only used in SNMP version 3. Indicates that authentication is used.
noauth	Only used in SNMP version 3. Indicates that no authentication is used.
priv	Only used in SNMP version 3. Indicates that privacy authentication is used.
<community>	Specifies the community string (used as a password) (16 characters maximum) for authorized agents to obtain access to SNMP information.
battery	Optional. Allows battery trap informs.
eps	Optional. Allows external power supply (EPS) informs.
rps	Optional. Allows redundant power supply (RPS) informs.
sfp	Optional. Allows small form-factor pluggable (SFP) informs.
snmp	Optional. Allows SNMP informs.
unit	Optional. Allows unit informs for user login/logout.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 13.1	Command was expanded to include the **informs** options.
Release R10.8.0	Command was expanded to include the **vrf** *<name>* parameter.
Release R10.9.0	Command was expanded to include the **eps** and **rps** parameters on the default VRF instance.
Release R11.11.0	Command was expanded to include the **battery** parameter.
Release R13.2.0	Command was expanded to include the **sfp** and **unit** parameters.
Release R13.3.0	Command was expanded to allow the *<name>* of a FQDN server to be specified as the recipient of SNMP information.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example sends all SNMP informs to the host at IPv4 address **190.3.44.69** and community string **MyCommunity** using SNMP **version 2c**:

(config)**#snmp-server host 190.3.44.69 informs version 2c MyCommunity snmp**

snmp-server host traps

Use the **snmp-server host traps** command to configure the unit to send traps to the specified SNMP host. Use the **no** form of this command to remove a specified host. Variations of this command include the following:

snmp-server host [<*ip address*> | <*name*>**] traps** <*community*>
snmp-server host [<*ip address*> | <*name*>**] traps version 1** <*community*> **[application] [battery] [bgp] [eps] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host [<*ip address*> | <*name*>**] traps version 2c** <*community*> **[application] [battery] [bgp] [eps] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host [<*ip address*> | <*name*>**] traps version 3 auth** <*community*> **[application] [battery] [bgp] [eps] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host [<*ip address*> | <*name*>**] traps version 3 noauth** <*community*> **[application] [battery] [bgp] [eps] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host [<*ip address*> | <*name*>**] traps version 3 priv** <*community*> **[application] [battery] [bgp] [eps] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [rps] [sfp] [snmp] [track] [unit] [voice] [vrrp]**

snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] traps** <*community*>
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] traps version 1** <*community*> **[application] [battery] [bgp] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] traps version 2c** <*community*> **[application] [battery] [bgp] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] traps version 3 auth** <*community*> **[application] [battery] [bgp] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] traps version 3 noauth** <*community*> **[application] [battery] [bgp] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [sfp] [snmp] [track] [unit] [voice] [vrrp]**
snmp-server host vrf <*name*> **[**<*ip address*> | <*name*>**] traps version 3 priv** <*community*> **[application] [battery] [bgp] [entity] [fan] [frame-relay] [network-sync] [over-temperature] [resource] [sfp] [snmp] [track] [unit] [voice] [vrrp]**

Syntax Description

<*ip address*>	Specifies the IP address (either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6)) of the SNMP host that receives the SNMP information. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal format X:X:X:X::X, for example, **2001:DB8:1::1**.

<name>	Specifies the Fully Qualified Domain Name (FQDN) (e.g., **adtran.com**) of the SNMP host that receives the SNMP information.
traps	Enables traps to this host. If the version is not specified, version 1 is used.
vrf *<name>*	Optional. Specifies the VRF instance on which the host exists. If a VRF instance is not specified, the default unnamed VRF is assumed.
version 1	Specifies using SNMP version 1 security model.
version 2c	Specifies using SNMP version 2c security model.
version 3	Specifies using SNMP version 3 user-based security model (USM).
auth	Only used in SNMP version 3. Indicates that authentication is used.
noauth	Only used in SNMP version 3. Indicates that no authentication is used.
priv	Only used in SNMP version 3. Indicates that privacy authentication is used.
<community>	Specifies the community string (used as a password) (16 characters maximum) for authorized agents to obtain access to SNMP information.
application	Optional. Allows application traps (such as, Domain Naming System (DNS) traps).
battery	Optional. Enables battery status traps.
bgp	Optional. Allows Border Gateway Protocol (BGP) traps.
entity	Optional. Enables the entity sensor traps such as insertion and deletion of a small form-factor pluggable (SFP) interface module.
eps	Optional. Allows external power supply (EPS) traps.
fan	Optional. Enables the fan failure notification traps.
frame-relay	Optional. Allows Frame Relay traps.
network-sync	Optional. Enables the network synchronization notification traps.
over-temperature	Optional. Enables the over-temperature protection traps.
resource	Optional. Enables the resource utilization set of traps.
rps	Optional. Allows redundant power supply (RPS) traps.
sfp	Optional. Allows small form-factor pluggable (SFP) traps.
snmp	Optional. Allows SNMP traps.
unit	Optional. Allows unit traps for user login/logout.
track	Optional. Allows the network monitor track traps.
voice	Optional. Allows voice traps.
vrrp	Optional. Allows Virtual Router Redundancy Protocol version 2 (VRRPv2) and version 3 (VRRPv3) traps.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 17.6	Command was expanded to include the **frame-relay** parameter.
Release 17.9	Command was expanded to include more **frame-relay** options, more **snmp** options, and the **voice** parameter. In addition, the **snmp-server host** <*ip address*> **traps version 3 priv** <*community*> version of the command was removed.
Release A2.04	Command was expanded to include **resource** traps.
Release 18.1	Command was expanded to include the **bgp** and **track** parameter.
Release R10.4.0	Command was expanded to include the **application** parameter.
Release R10.8.0	Command was expanded to include the **eps**, **rps**, and **vrf** <*name*> parameter.
Release R10.11.0	Command was expanded to include **entity, fan**, and **network-sync** traps.
Release R11.3.0	Command was expanded to include **vrrp** traps.
Release R11.6.0	Command was expanded to include **over-temperature** protection.
Release R11.11.0	Command was expanded to include **battery** traps.
Release R13.2.0	Command was expanded to include **sfp** and **unit** parameters.
Release R13.3.0	Command was expanded to allow the <*name*> of a FQDN server to be specified as the recipient of SNMP information.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example sends all SNMP traps to the host at IPv4 address **190.3.44.69** and sets the community string to **MyCommunity** using SNMP **version 2c**:

(config)**#snmp-server host 190.3.44.69 traps version 2c MyCommunity snmp**

snmp-server inform

Use the **snmp-server inform** command to set the number of retry attempts for a response and set the amount of time to wait for a response before allowing a new request. Use the **no** form of this command to return to the default setting. Variations of this command include the following:

snmp-server inform retries <*number*>
snmp-server inform timeout <*value*>

Syntax Description

retries <*number*>	Specifies number of retries for a response. The range is from **1** to **100**.
timeout <*value*>	Specifies time (in seconds) to wait for a response. The range is from **1** to **1000** seconds.

Default Values

By default, the retry count is set to 3 and the timeout is set to 5 seconds.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example sets the retry count to **10**:

(config)**#snmp-server inform retries 10**

snmp-server location *“<string>”*

Use the **snmp-server location** command to specify the Simple Network Management Protocol (SNMP) system location string. Use the **no** form of this command to return to the default value.

Syntax Description

“<string>”	Populates the system location string using an alphanumeric string enclosed in quotation marks (up to 32 characters in length).

Default Values

By default, the **snmp-server location** is set to **Adtran**.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a location of **5th Floor Network Room**:

(config)**#snmp-server location “5th Floor Network Room”**

snmp-server management-url *<url>*

Use the **snmp-server management-url** command to specify the uniform resource locator (URL) for the device's management software. Use the **no** form of this command to remove the management URL.

Syntax Description

<url>	Specifies the URL for the management software.

Default Values

By default, no URL is defined.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example specifies the URL **http://www.mywatch.com** as the device's management software:

(config)**#snmp-server management-url http://www.mywatch.com**

snmp-server management-url-label *<label>*

Use the **snmp-server management-url-label** command to specify a label for the uniform resource locator (URL) of the device's management software. Use the **no** form of this command to remove the label.

Syntax Description

<label>	Specifies a label for the URL of the management software (maximum length 255 characters).

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example specifies the label **watch** for the management software:

(config)**#snmp-server management-url-label watch**

snmp-server source-interface *<interface>*

Use the **snmp-server source-interface** command to specify a source interface for Simple Network Management Protocol (SNMP) traffic (including traps and get/set requests) originated by the unit. The IP address of the specified interface is used to source all SNMP traffic. The named Virtual Routing and Forwarding (VRF) instance further identifies the source interface when multiple VRF instances are configured on the router. Use the **no** form of this command to remove the specified interface.Variations of this command include:

snmp-server source-interface *<interface>*
snmp-server vrf *<name>* **source-interface** *<interface>*

Syntax Description

<interface>	Specifies the interface that should originate SNMP traffic. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **snmp-server source-interface ?** for a complete list of valid interfaces.
vrf *<name>*	Optional. Specifies the VRF instance on which the source interface exists.

Default Values

By default, there is no source-interface defined.

Command History

Release 7.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.8.0	Command was expanded to include the **vrf** <name> parameters.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned command without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example specifies that the **ethernet 0/1** on VRF **RED** should be the source for all SNMP traps and get/set requests:

(config)**#snmp-server vrf RED source-interface ethernet 0/1**

snmp-server user

Use the **snmp-server user** command to configure Simple Network Management Protocol (SNMP) users to control access to SNMP information. Use the **no** form of this command to remove a user from the specified SNMP server group. Variations of this command include:

snmp-server user <*username*> <*groupname*> **v1**
snmp-server user <*username*> <*groupname*> **v1 [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **v2c**
snmp-server user <*username*> <*groupname*> **v2c [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **v3**
snmp-server user <*username*> <*groupname*> **v3 [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **v3 auth md5** <*password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **v3 auth md5** <*password*> **priv des** <*password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **v3 auth sha** <*password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **v3 auth sha** <*password*> **priv des** <*password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**

NOTE *If **service password-encryption** is enabled, the running configuration changes to include the keyword **encrypted** before each password entry, which is masked. Refer to the command* *service password-encryption on page 1699**.*

Syntax Description

<*username*>	Specifies the name of the user.
<*groupname*>	Specifies the name of the group to which the user belongs.
v1	Specifies using the SNMP version 1 security model.
v2c	Specifies using the SNMP version 2c security model.
v3	Specifies using the SNMP version 3 (user-based) security model).
auth md5 <*password*>	Optional. Uses the HMAC-MD5-96 authentication level and a password string to build the key for the authentication level.
auth sha <*password*>	Optional. Uses the HMAC-SHA-96 authentication level and a password string to build the key for the authentication level.
priv des <*password*>	Optional. Uses the CBC-DES privacy authentication algorithm and a password string used for data encryption between the host and agent.
ip access-class <*ipv4 acl*>	Optional. Specifies an Internet Protocol version 4 (IPv4) access control list (ACL) entry.
ipv6 access-class <*ipv6 acl*>	Optional. Specifies an Internet Protocol version 6 (IPv6) ACL entry.

any-vrf	Optional. Specifies the ACL is applied to any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Specifies the ACL is applied to a specific VRF instance. If no VRF is provided, the default unnamed VRF is assumed.

It is necessary to configure the SNMP engine ID before configuration of the remote users for a particular agent can be completed. Refer to the command *snmp-server engineID remote on page 1797* *for instructions in setting the engine ID with the remote option.*

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 18.2	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran internetworking products only.
Release R10.1.0	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran voice products.
Release R10.8.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

The **snmp-server user** command can specify up to two ACLs to control access, one each for IPv4 and IPv6 protocols. When two ACLs are used, they must use the same VRF restriction (the default VRF, any VRF, or a specific VRF.) If no VRF is named, the default unnamed VRF is assumed.

Usage Examples

The following example enters a new user named **BobbyW** and assigns the user to a group called **securityV3auth** using version 3 security model, message digest 5 (MD5) authentication method with a password of **passWORD6243**, and no ACL to verify:

(config)#**snmp-server user BobbyW securityV3auth v3 auth md5 passWORD6243**

Technology Review

SNMP server users are configured and attached to a specified group with an SNMP version. The SNMP version defines the security model of the group, with SNMP version 1 (SNMPv1) being the least secure and SNMP version 3 (SNMPv3) the most secure. Groups also define the read, write, notify, and view access for each user that resides in the group.

Trap notifications in SNMP v1 and SNMP version 2 (SNMPv2) are sent once and do not require an acknowledgement upon receipt. With SNMPv3, a new form of notification type was introduced, called an inform. Unlike a trap sent with SNMPv1/v2, an inform requires a response be sent to the originating entity. If the originator of the inform notification does not receive the response before a specified timeout, the originator can resend until an acknowledgement response is received or a specified retry value is reached. Sending informs requires that the originator of the inform know the user, engine ID, security parameters, and belong to a group that grants access to the information.

SNMPv3 uses services, such as authentication, privacy, and ACLs to provide a higher level of security not present with v1 or v2. Of these new services, identifying an SNMP server user on a remote entity is necessary to receive and originate notifications, and also to generate and respond to commands.

snmp-server user <*username*> <*groupname*> remote <*host*> v3

Use the **snmp-server user remote v3** command to configure Simple Network Management Protocol version 3 (SNMPv3) users residing on a remote SNMP entity, to control access to SNMP information. The named Virtual Routing and Forwarding (VRF) instance further identifies the remote entity when multiple VRF instances are configured on the router. Use the **no** form of this command to remove a user from the specified SNMP group. Variations of this command include:

snmp-server user <*username*> <*groupname*> **remote** <*host*> **v3**
snmp-server user <*username*> <*groupname*> **remote** <*host*> **v3 [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote** <*host*> **v3 auth md5** <*auth password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote** <*host*> **v3 auth md5** <*auth password*> **priv des** <*priv password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf <name>]**
snmp-server user <*username*> <*groupname*> **remote** <*host*> **v3 auth sha** <*auth password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote** <*host*> **v3 auth sha** <*auth password*> **priv des** <*priv password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote vrf** <*vrf name*> <*host*> **v3**
snmp-server user <*username*> <*groupname*> **remote vrf** <*vrf name*> <*host*> **v3 [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote vrf** <*vrf name*> <*host*> **v3 auth md5** <*auth password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote vrf** <*vrf name*> <*host*> **v3 auth md5** <*auth password*> **priv des** <*priv password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote vrf** <*vrf name*> <*host*> **v3 auth sha** <*auth password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote vrf** <*vrf name*> <*host*> **v3 auth sha** <*auth password*> **priv des** <*priv password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**

*If **service password-encryption** is enabled, the running configuration changes to include the keyword **encrypted** before each password entry, which is masked. Refer to the command* *service password-encryption on page 1699**.*

Syntax Description

<*username*>	Specifies the name of the user.
<*groupname*>	Specifies the name of the group to which the user belongs.

<host>	Identifies the host name or Internet Protocol version4 (IPv4) or Internet Protocol version 6 (IPv6) address of a remote SNMP entity to which the user belongs. The remote host is necessary for acknowledgement of SNMP version 3 notifications. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv6 addresses should be expressed in colon hexadecimal format X:X:X:X::X, for example, **2001:DB8:1::1**.
vrf *<vrf name>*	Optional. When used after the **remote** keyword, specifies the remote host exists on the named VRF. If no VRF is provided, the default unnamed VRF is assumed.
v3	Uses SNMP version 3 (user-based security model).
auth md5 *<auth password>*	Optional. Uses the HMAC-MD5-96 authentication level and a password string to build the key for the authentication level.
auth sha *<auth password>*	Optional. Uses the HMAC-SHA-96 authentication level and a password string to build the key for the authentication level.
priv des *<priv password>*	Optional. Uses the CBC-DES privacy authentication algorithm and a password string used for data encryption between the host and agent.
ip access-class *<ipv4 acl>*	Optional. Specifies an Internet Protocol version 4 (IPv4) access control list (ACL) entry.
ipv6 access-class *<ipv6 acl>*	Optional. Specifies an Internet Protocol version 6 (IPv6) ACL entry.
any-vrf	Optional. Specifies the ACL is applied to any virtual routing and forwarding (VRF) instance.
vrf *<name>*	Optional. Specifies the ACL is applied to a specific VRF instance. If no VRF is provided, the default unnamed VRF is assumed.

It is necessary to configure the SNMP engine ID before configuration of the remote users for a particular agent can be completed. Refer to the command *snmp-server engineID remote on page 1797* *for instructions in setting the engine ID with the remote option.*

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 14.1	Command was expanded to include the **remote** *<host>* parameter.
Release 18.2	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran internetworking products only.
Release R10.1.0	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran voice products.

Release R10.8.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned command without specifying a VRF will only affect the default unnamed VRF.

The **snmp-server user** command can specify up to two ACLs to control access, one each for IPv4 and IPv6 protocols. When two ACLs are used, they must use the same VRF restriction (the default VRF, any VRF, or a specific VRF.) If no VRF is named, the default unnamed VRF is assumed.

When configuring a remote engine ID with a VRF specified, a remote user with the same host address and VRF must be configured.

Usage Examples

The following example enters a new user named **BobbyW** and assigns the user to a group called **securityV3auth** on the remote host at IPv4 address **198.168.1.3**, using version 3 security model, message digest 5 (MD5) authentication method with a password of **passWORD6243**, and no ACL to verify:

(config)**#snmp-server user BobbyW securityV3auth remote 198.168.1.3 v3 auth md5 passWORD6243**

Technology Review

SNMP server users are configured and attached to a specified group with an SNMP version. The SNMP version defines the security model of the group, with SNMP version 1 (SNMPv1) being the least secure and SNMP version 3 (SNMPv3) the most secure. Groups also define the read, write, notify, and view access for each user that resides in the group.

Trap notifications in SNMP v1 and SNMP version 2 (SNMPv2) are sent once and do not require an acknowledgement upon receipt. With SNMPv3, a new form of notification type was introduced, called an inform. Unlike a trap sent with SNMPv1/v2, an inform requires a response be sent to the originating entity. If the originator of the inform notification does not receive the response before a specified timeout, the originator can resend until an acknowledgement response is received or a specified retry value is reached. Sending informs requires that the originator of the inform know the user, engine ID, security parameters, and belong to a group that grants access to the information.

SNMPv3 uses services, such as authentication, privacy, and ACLs to provide a higher level of security not present with v1 or v2. Of these new services, identifying an SNMP server user on a remote entity is necessary to receive and originate notifications, and also to generate and respond to commands.

Remote users are specified with an IP address or port number for the remote SNMP entity where the user resides. Configuration of the SNMP remote engine ID is necessary before SNMPv3 inform notifications can be acknowledged. This is accomplished using the **snmp-server engineID remote** command. The remote entity's SNMP engine ID is used for password authentication and privacy digests. The configuration acknowledgments of informs will fail if the remote engine ID is not configured first. A management device must know about the user, the engine ID of the device, and security parameters, such as authentication, passwords, and security level in order for the command to be processed by the receiving agent.

snmp-server user <*username*> <*groupname*> remote auto-link v3

Use the **snmp-server user remote auto-link v3** command to configure Simple Network Management Protocol version 3 (SNMPv3) users residing on a remote SNMP entity, to control access to SNMP information. The remote SNMP device Internet Protocol version 4(IPv4) address follows the active auto-link server. Refer to the command *auto-link on page 1214* for more information on enabling auto-link. Use the **no** form of this command to remove a user from the specified SNMP group. Variations of this command include:

snmp-server user <*username*> <*groupname*> **remote auto-link v3**
snmp-server user <*username*> <*groupname*> **remote auto-link v3 [ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote auto-link v3 auth md5** <*auth password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote auto-link v3 auth md5** <*auth password*> **priv des** <*priv password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote auto-link v3 auth sha** <*auth password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**
snmp-server user <*username*> <*groupname*> **remote auto-link v3 auth sha** <*auth password*> **priv des** <*priv password*> **[ip access-class** <*ipv4 acl*> **| ipv6 access-class** <*ipv6 acl*>**] [any-vrf | vrf** <*name*>**]**

*If **service password-encryption** is enabled, the running configuration changes to include the keyword **encrypted** before each password entry, which is masked. Refer to the command service password-encryption on page 1699.*

Syntax Description

<*username*>	Specifies the name of the user.
<*groupname*>	Specifies the name of the group the user belongs to.
remote auto-link	Specifies that the remote SNMP device IPv4 address follows the active auto-link server.
v3	Uses SNMP version 3 (user-based security model).
auth md5 <*auth password*>	Optional. Uses the HMAC-MD5-96 authentication level and a password string to build the key for the authentication level.
auth sha <*auth password*>	Optional. Uses the HMAC-SHA-96 authentication level and a password string to build the key for the authentication level.
priv des <*priv password*>	Optional. Uses the CBC-DES privacy authentication algorithm and a password string used for data encryption between the host and agent.
ip access-class <*ipv4 acl*>	Optional. Specifies an Internet Protocol version 4 (IPv4) access control list (ACL) entry.
ipv6 access-class <*ipv6 acl*>	Optional. Specifies an Internet Protocol version 6 (IPv6) ACL entry.
any-vrf	Optional. Specifies the ACL is applied to any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Specifies the ACL is applied to a specific VRF instance. If no VRF is provided, the default unnamed VRF is assumed.

It is necessary to configure the SNMP engine ID before configuration of the remote users for a particular agent can be completed. Refer to the command snmp-server engineID remote on page 1797 for instructions in setting the engine ID with the remote option.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release 14.1	Command was expanded to include the **remote** <*host*> parameter.
Release 18.2	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran internetworking products only.
Release R10.1.0	Command syntax was changed to include the **ip access-class** and **ipv6 access-class** parameters for IPv6 support in Adtran voice products.
Release R10.8.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned command without specifying a VRF will only affect the default unnamed VRF.

The **snmp-server user** command can specify up to two ACLs to control access, one each for IPv4 and IPv6 protocols. When two ACLs are used, they must use the same VRF restriction (the default VRF, any VRF, or a specific VRF.) If no VRF is named, the default unnamed VRF is assumed.

When configuring a remote engine ID with a VRF specified, a remote user with the same host address and VRF must be configured.

Usage Examples

The following example enters a new user named **BobbyW** and assigns the user to a group called **securityV3auth** using version 3 security model on a remote auto-link server and authentication method message digest 5 (MD5) with a password of **passWORD6243** and no ACL to verify:

(config)**#snmp-server user BobbyW securityV3auth remote auto-link v3 auth md5 passWORD6243**

Technology Review

SNMP server users are configured and attached to a specified group with an SNMP version. The SNMP version defines the security model of the group, with SNMP version 1 (SNMPv1) being the least secure and SNMP version 3 (SNMPv3) the most secure. Groups also define the read, write, notify, and view access for each user that resides in the group.

Trap notifications in SNMP v1 and SNMP version 2 (SNMPv2) are sent once and do not require an acknowledgement upon receipt. With SNMPv3, a new form of notification type was introduced, called an inform. Unlike a trap sent with SNMPv1/v2, an inform requires a response be sent to the originating entity. If the originator of the inform notification does not receive the response before a specified timeout, the originator can resend until an acknowledgement response is received or a specified retry value is reached. Sending informs requires that the originator of the inform know the user, engine ID, security parameters, and belong to a group that grants access to the information.

SNMPv3 uses services, such as authentication, privacy, and ACLs to provide a higher level of security not present with v1 or v2. Of these new services, identifying an SNMP server user on a remote entity is necessary to receive and originate notifications, and also to generate and respond to commands.

Remote users are specified with an IP address or port number for the remote SNMP entity where the user resides. Configuration of the SNMP remote engine ID is necessary before SNMPv3 inform notifications can be acknowledged. This is accomplished using the **snmp-server engineID remote** command. The remote entity's SNMP engine ID is used for password authentication and privacy digests. The configuration acknowledgments of informs will fail if the remote engine ID is not configured first. A management device must know about the user, the engine ID of the device, and security parameters, such as authentication, passwords, and security level in order for the command to be processed by the receiving agent.

snmp-server view <*name*> <*value*>

Use the **snmp-server view** command to create or modify a Simple Network Management Protocol (SNMP) view entry. Use the **no** form of this command to remove an entry. Variations of this command include:

snmp-server view <*name*> <*value*> **excluded**
snmp-server view <*name*> <*value*> **included**

Syntax Description

<*name*>	Specifies a label for the view record being created. The name is a record reference.
<*value*>	Specifies the object identifier (OID) to include or exclude from the view. To identify the subtree, specify a string using numbers, such as 1.4.2.6.8. Replace a single subidentifier with the asterisk (*) to specify a subtree family.
excluded	Specifies a view to be excluded.
included	Specifies a view to be included.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.

Usage Examples

The **snmp-server view** command can include or exclude a group of OIDs. The following example shows how to create a view (named **blockInterfaces**) to exclude the OID subtree family **1.3.3.1.2.1.2**:

(config)**#snmp-server view blockInterfaces 1.3.3.1.2.1.2.* excluded**

The following example shows how to create a view (named **block**) to include a specific OID:

(config)**#snmp-server view block 1.3.3.1.2.1.2. included**

sntp retry-timeout <*value*>

Use the **sntp retry-timeout** command to set the amount of time to wait for a response before allowing a new request. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies time (in seconds) to wait for a response before retrying. The range is from **3** to **2000000** seconds.

Default Values

By default, the retry timeout is set to **5** seconds.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example sets the Simple Network Time Protocol (SNTP) retry timeout to **10** seconds:

(config)**#sntp retry-timeout 10**

sntp server

Use the **sntp server** command to set the host name of the Simple Network Time Protocol (SNTP) server, as well as the version of SNTP to use. SNTP is an abbreviated version of the Network Time Protocol (NTP). SNTP is used to set the time of the AOS product over a network. The SNTP server usually serves the time to many devices within a network. Use the **no** form of this command to return to the default setting. Variations of this command include:

sntp server [<*hostname*> **|** <*ip address*>**]**
sntp server [<*hostname*> **|** <*ip address*>**] version** <*number*>

Syntax Description

<*hostname*>	Specifies the host name of the SNTP server.
<*ip address*>	Specifies the IP address of the SNTP server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
version <*number*>	Optional. Specifies which NTP version is used. Valid range is **1** to **3**.

Default Values

By default, NTP version is set to **1**.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example sets the SNTP server to **time.nist.gov** using SNTP version 1 (the default version):

(config)**#sntp server time.nist.gov**

The following example sets the SNTP server as **time.nist.gov**. All requests for time use version 2 of the SNTP:

(config)**#sntp server time.nist.gov version 2**

sntp wait-time <*value*>

Use the **sntp wait-time** command to set the time between updates from the time server. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies time (in seconds) between updates. Range is **10** to **2000000** seconds.

Default Values

By default, the wait time is set to **86400** seconds (1 day).

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example sets the Simple Network Time Protocol (SNTP) wait time to two days:

(config)**#sntp wait-time 172800**

spanning-tree edgeport bpdufilter default

Use the **spanning-tree edgeport bpdufilter default** command to enable the bridge protocol data unit (BPDU) filter on all ports by default. Use the **no** form of this command to disable the setting.

Syntax Description

No subcommands.

Default Values

By default, **spanning-tree edgeport bpdufilter default** is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The BPDU filter blocks any BPDUs from being transmitted and received on an interface. This can be overridden on an individual port.

Usage Examples

The following example enables the bpdufilter on all ports by default:

(config)**#spanning-tree edgeport bpdufilter default**

To disable the BPDU filter on a specific interface, issue the appropriate commands for the given interface using the following commands as an example:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#spanning-tree edgeport bpdufilter disable**

spanning-tree edgeport bpduguard default

Use the **spanning-tree edgeport bpduguard default** command to enable the bridge protocol data unit (BPDU) guard on all ports by default. Use the **no** form of this command to disable the setting.

Syntax Description

No subcommands.

Default Values

Disabled by default.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpduguard blocks any BPDUs from being received on an interface. This can be overridden on an individual port.

Usage Examples

The following example enables the BPDU guard on all ports by default.

(config)**#spanning-tree edgeport bpduguard default**

To disable the BPDU guard on a specific interface, issue the appropriate commands for the given interface using the following commands as an example:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#spanning-tree edgeport bpduguard disable**

spanning-tree edgeport default

Use the **spanning-tree edgeport default** command to configure all ports to be edgeports by default. Use the **no** form of this command to disable the setting. This command is overridden by the spanning-tree edgeport command configured in the interface configuration mode.

Syntax Description

No subcommands.

Default Values

Disabled by default.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures all interfaces running spanning tree to be edgeports by default:

(config)**#spanning-tree edgeport default**

An individual interface can be configured to not be considered an edgeport. For example:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#spanning-tree edgeport disable**

or

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#no spanning-tree edgeport**

spanning-tree edgeport rootguard default

Use the **spanning-tree edgeport rootguard default** command to enable root guard on all interfaces configured as an edgeport. Use the **no** form of this command to disable the setting.

Syntax Description

No subcommands.

Default Values

Disabled by default.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Root guard blocks an interface from being elected to the root port role. If information about a superior root bridge is received, the interface will no longer forward traffic until superior root bridge proposals stop. If an interface has bridge protocol data unit (BPDU) filter or BPDU guard configured, configuring root guard will have no effect on the operation of the interface. The root guard setting can be overridden on an individual port basis.

Usage Examples

The following example enables the root guard on all ports by default.

(config)**#spanning-tree edgeport rootguard default**

To disable the root guard on a specific interface, issue the appropriate commands for the given interface. The following example disables the root guard on the gigabit switchport interface 0/3:

(config)**#interface gigabit-switchport 0/3**
(config-giga-swx 0/3)**#spanning-tree edgeport rootguard disable**

spanning-tree forward-time *<value>*

Use the **spanning-tree forward-time** command to specify the delay interval (in seconds) when forwarding spanning-tree packets. Use the **no** form of this command to return to the default interval.

Syntax Description

<value>	Specifies the forwarding delay interval in seconds. Range is **4** to **30** seconds.

Default Values

By default, the forwarding delay is set to **15** seconds.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the forwarding time to **18** seconds:

(config)#**spanning-tree forward-time 18**

spanning-tree hello-time <*value*>

Use the **spanning-tree hello-time** command to specify the delay interval (in seconds) between hello bridge protocol data units (BPDUs). To return to the default interval, use the **no** form of this command.

Syntax Description

<*value*>	Specifies the delay interval (in seconds) between hello BPDUs. Range is **0** to **1000000** seconds.

Default Values

By default, the delay is set to **2** seconds.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures a **spanning-tree hello-time** interval of **10000** seconds:

(config)#**spanning-tree hello-time 10000**

spanning-tree max-age *<value>*

Use the **spanning-tree max-age** command to specify the interval (in seconds) the spanning tree will wait to receive bridge protocol data units (BPDUs) from the root bridge before assuming the network has changed (thus re-evaluating the spanning-tree topology). Use the **no** form of this command to return to the default interval.

Syntax Description

<value>	Specifies the wait interval (in seconds) between received BPDUs (from the root bridge). Range is **6** to **40** seconds.

Default Values

By default, the wait interval is set at **20** seconds.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures a wait interval of **35** seconds:

(config)**#spanning-tree max-age 35**

spanning-tree mode

Use the **spanning-tree mode** command to choose a spanning tree mode of operation. Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree mode rstp
spanning-tree mode stp

Syntax Description

rstp	Enables Rapid Spanning Tree Protocol (RSTP).
stp	Enables spanning-tree protocol.

Default Values

By default, **spanning-tree mode** is set to **rstp**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the spanning-tree mode to **rstp**:

(config)**#spanning-tree mode rstp**

spanning-tree pathcost method

Use the **spanning-tree pathcost method** command to select a short or long pathcost method used by the spanning-tree protocol. Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree pathcost method long
spanning-tree pathcost method short

Syntax Description

long	Specifies a long pathcost method.
short	Specifies a short pathcost method.

Default Values

By default, **spanning-tree pathcost** is set to **short**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example specifies that the spanning-tree protocol use a **long** pathcost method:

(config)**#spanning-tree pathcost method long**

spanning-tree priority <*value*>

Use the **spanning-tree priority** command to set the priority for spanning-tree interfaces. The lower the priority value, the higher the likelihood the configured spanning-tree interface will be the root for the bridge group. To return to the default bridge priority value, use the **no** form of this command.

Syntax Description

<*value*>	Sets a priority value for the bridge interface. Configuring this value to a low number increases the interface's chance of being the root. Therefore, the maximum priority level would be 0. Range is **0** to **65535**.

Default Values

By default, the priority level is set to **32768**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets **spanning-tree priority** to the maximum level:

(config)**#spanning-tree priority 0**

srtp-profile *<profile name>*

Use the **srtp-profile** command to enter the Secure Realtime Transfer Protocol (SRTP) Profile Configuration mode, from which the operation of SRTP is configured. Use the **no** form of this command to remove the profile.

Syntax Description

<profile name>	Specifies the name of the SRTP profile to create.

Default Values

By default, no SRTP profiles exist.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Each entity on the AOS device that uses SRTP must have an SRTP profile applied in order to function. Many SRTP profiles can exist and be referenced by many entities using SRTP on the AOS device. The same SRTP profile can be used by as many entities using SRTP as required. The SRTP profile essentially operates as a template for SRTP operation and is applied on a per-trunk basis. For more information regarding SRTP configuration, refer to the *SRTP Profile Command Set on page 4888*.

Usage Examples

The following example creates the SRTP profile **SRTPPROFILE1** and enters the profile's configuration mode:

```
(config)#srtp-profile SRTPPROFILE1
(config-srtp-profile-SRTPPROFILE1)#
```


ssh-server <*TCP port*>

Use the **ssh-server** command to specify an alternate Transmission Control Protocol (TCP) port for secure shell (SSH) servers. Use the **no** form of this command to return to the default setting.

Syntax Description

<*port*>	Specifies the alternate TCP port for the SSH server.

Default Values

By default, the SSH server listens on TCP port **22**.

Command History

Release 18.2	Command was introduced. This command replaces the **ip ssh-server** <*port*> command for Adtran internetworking products only.
Release R10.1.0	Command was introduced. This command replaces the **ip ssh-server** <*port*> command for Adtran voice products.
Release R14.4.0	Command was introduced. This command is used to specify an alternate TCP port.

Functional Notes

SSH is a version of Telnet that allows you to run command line and graphical applications (as well as, transfer files) over an encrypted connection.

Usage Examples

The following example configures the SSH server to listen on TCP port **2200**, instead of the default port **22**:

(config)**#ip ssh-server 2200**

To return to the default setting, use the **no** form of the command. For example:

(config)**#no ip ssh-server 2200**

ssh-server authentication

Use the **ssh-server authentication** command to enable password and/or public key authentication for secure shell (SSH) connections to the system. Use the **no** form of this command to return to the default. Variations of this command include:

ssh-server authentication password
ssh-server authentication password pubkey
ssh-server authentication pubkey
ssh-server authentication pubkey password

Syntax Description

password	Allows password authentication for SSH connections.
pubkey	Allows public key authentication for SSH connections.

Default Values

By default, both password and pubkey authentication are enabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables public key authentication for SSH connections on the system:

>**enable**

#configure terminal

(config)**#ssh-server authentication password pubkey**

ssh-server cipher

Use the **ssh-server cipher** command to configure the secure shell (SSH) server cipher algorithm used in SSH connections to the system. Use the **no** form of this command to disable a cipher. Variations of this command include:

ssh-server cipher 3des-cbc
ssh-server cipher aes128-ctr
ssh-server cipher aes256-ctr

Syntax Description

3des-cbc	Enables 3des-cbc as a supported cipher for SSH connections.
aes128-ctr	Enables aes128-ctr as a supported cipher for SSH connections.
aes256-ctr	Enables aes256-ctr as a supported cipher for SSH connections.

Default Values

By default, **taes128-ctr** and **aes256-ctr** are enabled and **3des-cbc** is disabled.

Command History

Release R13.12.0	Command was introduced.

Usage Examples

The following example disables aes128-ctr for SSH connections on the system:

>**enable**

#configure terminal

(config)**#ssh-server cipher aes128-ctr**

ssh-server host-key

Use the ssh-server ssh-host-key command to configure the SSH server host-key algorithm used in SSH connections to the system. Use the **no** form of this command to disable an algorithm. Variations of this command include:

ssh-server host-key <*input*>

Syntax Description

host-key	Specifies the SSH client host-key algorithm.
ecdsa -sha2-nistp256	Enables ecdsa-sha2-nistp256 host key signature algorithm for signing and verifying sha256 message hash for securing SSH connections
ecdsa -sha2-nistp384	Enables ecdsa-sha2-nistp384 host key signature algorithm for signing and verifying sha256 message hash for securing SSH connections
ecdsa -sha2-nistp521	Enables ecdsa-sha2-nistp521 host key signature algorithm for signing and verifying sha256 message hash for securing SSH connections
rsa-sha2-512	Enables rsa-sha2-512 host key signature algorithm for signing and verifying sha512 message hash for securing SSH connections.
ssh-dss	Enables ssh-dss host key algorithm for signing and verifying sha1 message hash for securing SSH connections.
ssh-rsa	Enables ssh-rsa host key algorithm for signing and verifying sha1 message hash for securing SSH connections.

Default Values

By default ssh-rsa, ssh-dss are enabled, and rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp521, ecdsa-sha2-nistp384 are disabled.

Command History

Release 14.4.0	Command was introduced.

Usage Examples

The following example configures various SSH client host-key algorithms.

>**enable**
#configure terminal
(config)**#ssh-server host-key ecdsa-sha2-nistp256**
(config)**#ssh-server host-key ecdsa-sha2-nistp384**
(config)**#ssh-server host-key ecdsa-sha2-nistp521**
(config)**#ssh-server host-key rsa-sha2-512**
(config)**#ssh-server host-key ssh-dss**
(config)**#ssh-server host-key ssh-rsa**

ssh-server kex

Use the **ssh-server kex** command to configure the secure shell (SSH) server key exchange (KEX) algorithm used in SSH connections to the system. Use the **no** form of this command to disable an algorithm. Variations of this command include:

ssh-server kex diffie-hellman-group-exchange-sha256
ssh-server kex diffie-hellman-group1-sha1
ssh-server kex diffie-hellman-group14-sha1
ssh-server kex diffie-hellman-group16-sha512
ssh-server kex ecdh-sha2-nistp256

Syntax Description

diffie-hellman-group-exchange -sha256	Enables the Diffie-Hellman Group Exchange key exchange, with SHA256 as the hash, as supported key exchange method for SSH connections.
diffie-hellman-group1-sha1	Enables the Diffie-Hellman Group 1 key exchange, with SHA-1 as the hash, as a supported key exchange method for SSH connections.
diffie-hellman-group14-sha1	Enables the Diffie-Hellman Group 14 key exchange, with SHA-1 as the hash, as a supported key exchange method for SSH connections.
diffie-hellman-group16-sha512	Enables the Diffie-Hellman Group 16 key exchange, with SHA512 as the hash, as a supported key exchange method for SSH connections.
ecdh-sha2-nistp256	Enables ECDH algorithm with SHA2 as the hash, as a supported key exchange method for SSH connections.

Default Values

By default, diffie-hellman-group1-sha1, diffie-hellman-group16-sha512, diffie-hellman-group-exchange-sha256, ecdh-sha2-nistp256 kex are disabled, and diffie-hellman-group14-sha1 is enabled.

Command History

Release R13.12.0	Command was introduced.
Release R14.4.0	Command was expanded to include diffie-hellman-group16-sha512, diffie-hellman-group-exchange-sha256, and ecdh-sha2-nistp256 kex options.

Usage Examples

The following examples are used for SSH key exchange connections using diffie-hellman and ECDH algorithms.

>**enable**
#configure terminal
config)**#ssh-server kex diffie-hellman-group-exchange-sha256**
(config)**#ssh-server kex diffie-hellman-group1-sha1**
(config)**#ssh-server kex diffie-hellman-group14-sha1**
(config)**#ssh-server kex diffie-hellman-group16-sha512**
(config)**#ssh-server kex ecdh-sha2-nistp256**

ssh-server mac

Use the **ssh-server mac** command to configure the secure shell (SSH) server message authentication code (MAC) algorithm used in SSH connections to the system. Use the **no** form of this command to disable an algorithm. Variations of this command include:

ssh-server mac hmac-sha1
ssh-server mac hmac-sha2-256

Syntax Description

hmac-sha1	Enables SHA-1 hash-based MAC (HMAC) encryption for securing SSH connections.
hmac-sha2-256	Enables SHA-256 HMAC encryption for securing SSH connections.

Default Values

By default, the SHA-1 HMAC algorithm (**hmac-sha1**) is disabled and the SHA-256 HMAC algorithm (**hmac-sha2-256**) is enabled.

Command History

Release R13.12.0	Command was introduced.

Usage Examples

The following example disables SHA-1 HMAC algorithm for SSH connections on the system:

(config)**#no ssh-server mac hmac-sha1**

ssh-server moduli

Use the **ssh-server moduli** command to configure the SSH server moduli values.Variations of this command include:

ssh-server moduli min <1024/1536/2048/3072/4096/6144> max <1536/2048/3072/4096/6144>

Syntax Description

moduli min	Sets the minimum moduli value. Optional values are: <1024/1536/2048/3072/4096/6144>
moduli max	Sets the maximum moduli value. Optional values are: <1536/2048/3072/4096/6144/8192>

Default Values

By default, ssh-server moduli min is set to 1024 and max is set to 8192.

Command History

Release R14.4.0	Command was introduced.

Usage Examples

The **min** and **max** moduli values must correspond. For example, a **min** value of 1024 must have a corresponding **max** value of 1536, 2048, 3072, 4096, 6144 or 8192. The reverse is also necessary. Any **max** value must have a corresponding **min** value.

The following examples set the minimum and maximum moduli values.

>**enable**
#configure terminal
(config)**#ssh-server moduli min 1024 max 1536**
(config)**#ssh-server moduli min 1536 max 3072**
(config)**#ssh-server moduli min 2048 max 6144**

ssh-server pubkey-chain

Use the **ssh-server pubkey-chain** command to enter the secure shell (SSH) Server Public Key Configuration mode and configure the SSH public key chain for public key based authentication. From within the SSH Server Public Key Configuration mode, a public key can be added for a remote device to gain access to the system through SSH connection. Use the **no** form of this command to remove the public key. Once **ssh-server pubkey-chain** command is entered into the system, the username and key type must follow with a subsequent command. To enter the SSH Server Public Key Configuration mode, enter the command as follows:

#ssh-server pubkey-chain

The following subcommands are available once you enter the SSH Server Public Key Configuration mode:

username <*username*> **key-hash ecdsa-sha2-nistp<256/384/521>** <*input*>
username <*username*> **key-hash ssh-<dss/rsa>** <*input*>
username <*username*> **key-hash ssh-rsa-sha2-512>** <*input*>
username <*username*> **key-hash ssh-rsa** <*input*>
username <*username*> **key-string**
username <*username*> **key-string sha2**
username <*username*> **privilege** <*level*> **key-hash ssh-hash** <*input*>
username <*username*> **privilege** <*level*> **key-hash ssh-rsa** <*input*>
username <*username*> **privilege** <*level*> **key-string** <*input*> **sha2**

Syntax Description

username <*username*>	Specifies the username of a remote device user to allow access through SSH connections. Only one key per user is allowed.
key-hash	Specifies adding a public key hash (SHA1 hash of Digital Signature Standard (DSS) or Rivest-Shamir-Adleman (RSA) formats) for the specified user.
e**cdsa-sha-nistp256**	Specifies SHA2 hash of ECDSA hash of 256 format.
e**cdsa-sha-nistp384**	Specifies SHA2 hash of ECDSA hash of 384format.
e**cdsa-sha-nistp521**	Specifies SHA2 hash of ECDSA hash of 521 format.
ssh-dss	Specifies SHA1 hash of DSS format.
ssh-rsa	Specifies SHA1 hash of RSA format.
ssh-sa-sha2-512	Specifies the SSH hash of RSA format.
sha2	Specifies the SSH hash of RSA format.
key-string	Specifies using a public key string (DSS or RSA format) for the specified user. Key strings can be entered in either open SSH or PEM format.
privilege <*level*>	Optional. Specifies a privilege level for this user at the time of authentication. Valid entries are **1** to **7**.

Default Values

By default, there are no SSH users authorized to gain access to the system using public keys.

Command History

Release R10.10.0	Command was introduced.
Release R10.11.0	Command was expanded to include the **privilege** parameter.
Release R12.2.0	Command was expanded to include support for RSA keys.
Release R14.4.0	Command was expanded to include support for RSA keys.

Functional Notes

Users can have one or both (DSS or RSA) key types at any given time. The system can store up to 100 user keys on the system at a time.

Once the command **username** <*username*> **key-string** is entered, a prompt results requesting the key string for the user be entered. After entering the key string, press **Enter** twice or type **quit** on a single line to end this function and return to the Global Configuration mode.

Usage Examples

The following example adds a public key for the remote user **ALPHA1** using a key-string in openSSH format:

(config)**#ssh-server pubkey-chain**
(config-ssh-pubkey-chain)**#username ALPHA1 key-string sha2**
(config-ssh-pubkey-ALPHA1)#
Enter user's public key (DSS). End with two consecutive carriage returns or the word “quit” on a line by itself:
ssh-dss
AAAB3NzaC1kc3MAAACBAOLniJWw39O5IXjm83M0DKOAKKa8wEB0zhr1SCnESmrnipCRagU2W
GzTcr9npbD2OFpDrUFZf9VDItIjs+uR3yA8CbN52nS8ICOsVjjg7rnPUZb5giwPEir7WTICCe2g9ssRBJ
zXodn4X+2kGSwcDQhD2zsTs6o9sltT9AID65y9AAAAFQD8ADcvXx46s8lfRGPwfWgAlzGh0QAAAIA
qgGhQHe0jrgfTwdSxIr+pVCvHvW//eDoCa/M9/PrWnuCmV3oKpGAbqcbaHYnX0CxCY9qNguABiFfY
OTP9GDSy8PKXEg1praIEM21GTNtt3kZU9rH/ReZiMLXa6kPZDx4wTPfV3smEwKIWIvWFQypbdNZ
TSoJY7YKvezo+8J3fegAAAIApJW5seH5ume7mkmiI53LAKyfxrHu4CM3fI+kDQNTJg1YRoJkDEJ6KK
ph0D79xprl/i2SSJEkKHV2SEOr8Iu/vFx71xaZxWNbnkZwnMaDQGNYjUQJAioqN9IVi+HTnZ75yCU4x
h9HjbKt/S2UuEh9+s3cKdV37ohbDKyQruU9vhw== ALPHA1@sample.adtran.com

Success!

The following example adds a public key for the remote user **ALPHA1** using a key string in PEM format:

(config)**#ssh-server pubkey-chain**
(config-ssh-pubkey-chain)**#username ALPHA1 key-string**
(config-ssh-pubkey-ALPHA1)#
Enter the user’s public key (DSS). End with two consecutive carriage returns or the word “quit” on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----

Comment: "dsa-key-20130916"
AAAAB3NzaC1kc3MAAACBAKE3uUZO0sKCjQwtK+uTeAHexx2QpGU8nXxMJ4nCALIH
KVn0YRPOZtmSbutDrMHkCG2aBqT16KGs2l0pECD0KNNNp0ayuQCxJrd8UjDI8CA2
80GGc3lPdT3f18RLZEQRar1FYo4LFmYhA4DQkR46eJvvXLRia5uJlNysj6/QGMub
AAAAFQDZznKwiYd+CMOvSeYTJxHoUm3vOwAAAIEAi1N+eDtABpgACRffzIAypPdx
Flu2+VYtZWtPFgfyV8qNSAUUp/0e8U71BweQwBrypfaVrVOOKeuET1FxBqZZoAQa
eH/IMF+MxZ8MOW6krWwl+z8Jw9R9z+KlJUXmd1Tr1+oriKPmLidzd37jFXIufv5H
TiD1yzo18LeumBMxAeQAAACANJKNBR9NV6g6EF8o3AT91UcwFkXCIPJ8Tdgai7fB
REen0pSrg17ENWU5NTPhqMBb7aHjYrEre5TJNF0LZlSRAOwLVOFUPu3/GjVZ0iOE
yKSm6W08oGU5aoMhC/+nRUqaXScNRfh32UsAItJQGgtaIePTPHK3x53+bXY1fr3b
3L4=
---- END SSH2 PUBLIC KEY ----

Success!

The following example adds a public key for the remote user **CHARLIE3** using the hash key **A54568F4DA1BAB8BB53CF0ABD818FCDA**:

(config)**#ssh-server pubkey-chain**
(config-ssh-pubkey-chain)**#username CHARLIE3 key-hash ssh-dss**
A54568F4DA1BAB8BB53CF0ABD818FCDA
(config-ssh-pubkey-CHARLIE3)#

The following example removes the key string for the user **ALPHA1**:

(config-ssh-pubkey-ALPHA1)**#no ALPHA1 key-string**

The following example adds a privilege level 1 for the user **ALPHA**:

(config)**#ssh-server pubkey-chain**
(config-ssh-pubkey-chain)**#username ALPHA privilege 1 key-hash ssh-dss** *<key-hash for this user>*

ssh-server <TCP Port>

Use the **ssh-server TCP Port** command to listen on an alternate port. To access an alternate port, enter the command as follows:

#ssh-server port <*1-65535*>

Syntax Description

port <*1-65535*>	Specifies the alternate port.

Default Values

By default, there are no default values

Command History

Release R14.4.0	Command was expanded to include support for RSA keys.

Functional Notes

Usage Examples

The following example adds a TCP port:

>**enable**
#configure terminal
(config)**#ssh-server port** <*1-65535*>

ssh-client host-key

Use the ssh-client host-key command to configure the secure shell (SSH) client host-key algorithm used in SSH connections for the system. Use the **no** form of this command to disable an algorithm. Variations of this command include:

ssh-client host-key ecdsa-sha2-nistp256
ssh-client host-key ecdsa-sha2-nistp384
ssh-client host-key ecdsa-sha2-nistp521
ssh-client host-key ssh-dss
ssh-client host-key ssh-ed25519
ssh-client host-key ssh-rsa
ssh-client host-key ssh-rsa-sha2-256
ssh-client host-key ssh-rsa-sha2-512

Syntax Description

host-key	Specifies the SSH client host-key algorithm.
ecdsa -sha2-nistp256	Enables ecdsa-sha2-nistp256 host-key signature algorithm for signing and verifying sha256 hash for securing SSH connections.
ecdsa-sha2-nistp384	Enables ecdsa-sha2-nistp384 host-key signature algorithm for signing and verifying sha384 hash for securing SSH connections.
ecdsa-sha2-nistp521	Enables the ecdsa-sha2-nistp521 host-key signature algorithm for signing and verifying sha521 hash for securing SSH connections.
ssh-dss	Enables the ssh-dss host-key algorithm for signing and verifying sha1 message hash for securing SSH connections.
ssh-ed25519	Enables the ssh-ed25519 host-key algorithm for signing and verifying the SHA message hash for securing SSH connections.
ssh-rsa	Enables the ssh-rsa host-key algorithm for signing and verifying the SHA message hash for securing SSH connections.
ssh-rsa-sha2-256	Enables the ssh-rsa-sha2-256 host-key algorithm for signing and verifying the 256 message hash for securing SSH connections.
ssh-rsa-sha2-512	Enables the ssh-rsa-sha2-sha512 host-key signature algorithm for signing and verifying sha512 hash for securing SSH connections.

Default Values

By default, all the host-key algorithms are enabled and follows the following host-key priority order: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519, rsa-sha2-512, rsa-sha2-256, ssh-rsa, ssh-dss

Command History

Release 14.3.0	Command was introduced.

Usage Examples

The following example configures various SSH client host-key algorithms.

>**enable**
#configure terminal
(config)**#ssh-client host-key ssh-ecdsa-sha2-nistp256**
(config)**#ssh-client host-key ssh-ecdsa-sha2-nistp384**
(config)**#ssh-client host-key ecdsa-sha2-nistp521**
(config)**#ssh-client host-key ssh-dss**
(config)**#ssh-client host-key ed25519**
(config)**#ssh-client host-key ssh-rsa**
(config)**#ssh-client host-key-rsa-sha2-512**

ssh-client kex

Use the ssh-client kex command to configure the secure shell (SSH) client KEX algorithms used in SSH connections from the system. Use the **no** form of this command to disable an algorithm. Variations of this command include:

ssh-client kex diffie-hellman-group-exchange-sha1
ssh-client kex diffie-hellman-group-exchange-sha256
ssh-client kex diffie-hellman-group1-sha1
ssh-client kex diffie-hellman-group14-sha1
ssh-client kex ecdh-sha2-nistp256
ssh-client kex ecdh-sha2-nistp384
ssh-client kex ecdh-sha2-nistp521
ssh-client kex ssh-curve25519-sha256
ssh-client kex ssh-curve25519-sha256-libssh

Syntax Description

kex	Specifies the KEX client host-ey Exchange algorithms.
diffie-hellman-group-exchange-sha1	Enables the Diffie-Hellman Group Exchange key exchange, with **SHA1** as a hash, as a supported key exchange method for SSH connections.
diffie-hellman-group-exchange-sha256	Enables the Diffie-Hellman Group Exchange key exchange, with **SHA256** as a hash, as a supported key exchange method for SSH connections.
diffie-hellman-group1-sha1	Enables the Diffie-Hellman **Group1** key exchange, with **SHA-1** as a hash, as a supported key exchange method for SSH connections.
diffie-hellman-group1-sha14	Enables the Diffie-Hellman **Group14** key exchange, with **SHA-1** as a hash, as a supported key exchange method for SSH connections.
ecdh-sha2-nistp256	Enables Elliptic Curve Diffie-Hellman key exchange, with SHA256 as a hash, as a supported key exchange method for SSH connections.
ecdh-sha2-nistp384	Enables Elliptic Curve Diffie-Hellman key exchange, with SHA384 as a hash, as a supported key exchange method for SSH connections.
ecdh-sha2-nistp521	Enables Elliptic Curve Diffie-Hellman key exchange, with SHA521 as a hash, as a supported key exchange method for SSH connections.
ecdh-curve25519-sha256	Enables Elliptic Curve25519 key exchange, with SHA256 as a hash, as a supported key exchange method for SSH connections.
ecdh-curve25519-sha256-libssh	Enables Elliptic Curve25519-sha256@libssh key exchange, with SHA256 as a hash, as a supported key exchange method for SSH connections.

Default Values

By default, all the Key Exchange algorithms are enabled. The order of default priority is as follows:

ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1

Command History

Release 14.3.0	Command was introduced.

Usage Examples

The following examples configure various SSH client kex algorithms.

>**enable**
>**configure terminal**
(config)#ssh-client kex diffie-hellman-group-exchange-sha1
(config)#ssh-client kex diffie-hellman-group-exchange-sha256
(config)#ssh-client kex diffie-hellman-group1-sha1

stack

Use the **stack** command to configure switch-stacking options. Use the **no** form of this command to disable this feature. Variations of this command include:

stack master
stack master *<vlan id>*
stack master *<vlan id> <ip address> <subnet mask>*
stack member *<mac address>*
stack member *<mac address> <unit id>*
stack vlan *<vlan id>*

Syntax Description

master	Specifies that the unit will be the master of the stack.
<vlan id>	Specifies the virtual local area network (VLAN) ID the stack will use for communication.
<ip address>	Configures the network mask of the private IP network. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
member	Adds a switch to the stack.
<mac address>	Specifies a valid 48-bit medium access control (MAC) address of the unit being added. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
<unit id>	Specifies the unit ID of the switch being added.
vlan *<vlan id>*	Specifies the VLAN ID of the stack of which you are a member.

Default Values

By default, stack VLAN is **2386**, and the stack IP network is **169.254.0.0 /24**.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example configures the unit to be the stack master and use the default stack VLAN and IP network.

(config)**#stack master 2000**

The following example configures the unit to be the stack master and use VLAN 2000 as the management VLAN and 192.168.1.0 /24 as the management network.

(config)**#stack master 2000 192.168.1.0 /24**

The following example adds the switch with the CPU MAC address 00:A0:C8:00:8C:20 to the stack; also assigns the number 2 as the new stack member's unit ID.

(config)**#stack member 00:A0:C8:00:8C:20 2**

The following example specifies that this unit is in the stack using VLAN 2000 as its management VLAN; also specifies that this unit is in stack member mode (not a stack-master).

(config)**#stack vlan 2000**

statistics rate-interval <*value*>

Use the **statistics rate-interval** command to specify the interval (in seconds) to receive interface statistics. Use the **no** form of this command to return to the default interval.

Syntax Description

<*value*>	Specifies the wait interval. Range is **30** to **600** seconds (in 30 second increments).

Default Values

By default, the wait interval is set at **300** seconds.

Command History

Release 17.4	Command was introduced.

Usage Examples

The following example configures a wait interval of **90** seconds:

(config)**#statistics rate-interval 90**

system-control-evc

Use the **system-control-evc** command to enter the system control Ethernet virtual connection (EVC) configuration mode. This configuration mode is used for dynamic provisioning and to separate the session control Point-to-Point Protocol over Ethernet (PPPoE) interface from regular customer services.

Syntax Description

No subcommands.

Default Values

By default, the system control EVC is always activated.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

The configuration commands for the system control EVC are outlined in the *System Control EVC Command Set on page 3745*.

Usage Examples

The following example enters the system control EVC configuration mode:

```
(config)#system-control-evc
(config-sys-cntrl-evc)#
```


system-management-evc

Use the **system-management-evc** command to enter the System Management Ethernet Virtual Connection (EVC) Configuration mode. This configuration mode is used to configure an inband IP network interface for the purposes of system management and control. The configuration commands for the system management EVC are outlined in the *System Management EVC Command Set on page 3843*.

Syntax Description

No subcommands.

Default Values

By default, the system management EVC is always activated.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enters the system management EVC configuration mode:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#
```


system mtu *<size>*

Use the **system mtu** command to set the maximum transmission unit (MTU) size for all ports on the AOS device and allow Ethernet frames larger than 1518 bytes (known as jumbo frames) to pass. Use the **no** form of this command to return to the default.

Syntax Description

<size>	Indicates the transmission size in bytes. The valid range is 1518 to the maximum byte size allowed for the unit being configured.

The MTU size specified does not include an 802.1Q virtual local area network (VLAN) tag. For example, if the MTU size is set to allow 1518 bytes, an 802.1Q tagged packet of 1522 bytes would still be accepted.

Default Values

By default, the MTU size is **1518**.

Changing the default value (1518) in a switch already installed in a network could cause traffic disruption.

Command History

Release 17.6	Command was introduced.

Usage Examples

The following example sets the maximum transmission unit size for all ports on the device to **9216** bytes:

(config)**#system mtu 9216**

tacacs-server

Use the **tacacs-server** command to configure several terminal access controller access-control system plus (TACACS+) parameters for all TACACS+ servers on the network. Most of these global settings can be overridden on a per-server basis (using the command *tacacs-server host on page 1868*). Use the **no** form of this command to return to the default setting. Variations of this command include the following:

tacacs-server key <*key*>
tacacs-server packet maxsize <*value*>
tacacs-server timeout <*value*>

Syntax Description

key <*key*>	Specifies the encryption key used by all TACACS+ servers. This is a global setting; however, it can be overridden on a per-server basis.
packet maxsize <*value*>	Specifies the maximum packet size that can be sent to any TACACS+ server. Packet maxsize range is **10240** to **65535** kilobytes.
timeout <*value*>	Specifies the time (in seconds) that the AOS unit will wait for the server's reply before declaring an error. The time range is **1** to **1000** seconds. This is a global setting; however, it can be overridden on a per-server basis.

Default Values

By default, there is no key specified for TACACS+ servers, the packet maxsize is set to **10240** kb, and the TACACS+ server timeout is set to **5** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets a timeout limit of **60** seconds for all TACACS+ servers:

(config)**#tacacs-server timeout 60**

tacacs-server host

Use the **tacacs-server host** command to specify the parameters for a terminal access controller access-control system plus (TACACS+) server. Specifying the virtual routing and forwarding (VRF) instance using the **vrf** <*name*> keyword applies the configuration to the named VRF instance. Omitting the **vrf** <*name*> keyword applies the configuration to the TACACS+ server for the default unnamed VRF. Use the **no** form of this command to return to the default setting. Variations of this command include the following:

tacacs-server host <*hostname*> **|** <*ip address*>
tacacs-server host <*hostname*> **|** <*ip address*> **key** <*key*>
tacacs-server host <*hostname*> **|** <*ip address*> **port** <*port*>
tacacs-server host <*hostname*> **|** <*ip address*> **timeout** <*value*>
tacacs-server vrf <*name*> **host** <*hostname*> **|** <*ip address*>
tacacs-server vrf <*name*> **host** <*hostname*> **|** <*ip address*> **key** <*key*>
tacacs-server vrf <*name*> **host** <*hostname*> **|** <*ip address*> **port** <*port*>
tacacs-server vrf <*name*> **host** <*hostname*> **|** <*ip address*> **timeout** <*value*>

Each parameter after <hostname | ip address> specifies the characteristics of the individual TACACS+ server. Parameters can be entered in a single command line, in any order, but each may only be used once.

Syntax Description

<*hostname*> **|** <*ip address*>	Specifies the server to configure. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the AOS device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the command *name-server on page 1622*.
key <*key*>	Specifies the encryption key used by the TACACS+ server. This command overrides the global TACACS+ key setting (set with the command *tacacs-server on page 1867*). This command must be entered last in the command line because everything after the **key** parameter is read as the new key.
port <*port*>	Specifies the Transmission Control Protocol (TCP) port used by the TACACS+ server. Range is **1** to **65535**.
timeout <*value*>	Specifies the time to wait (in seconds) for the server to reply to requests. Range is **1** to **1000** seconds.
vrf <*name*>	Specifies the name of the VRF to which to assign the association. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, the TACACS+ server uses TCP port **49**. By default, the key and timeout values are the values set by the command *tacacs-server on page 1867*.

Command History

Release 11.1	Command was introduced.
Release R10.7.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

At a minimum, the address (IP or host name) of the server must be given. The other parameters can be entered in any order (except the **key** parameter) and, if the parameters are not specified, they will take default values or fall back on the global TACACS+ server's default settings (set using the command *tacacs-server on page 1867*).

If global password protection is enabled on the AOS device, encryption will be applied to the authentication key (**key** <*key*>). If global password protection is off, the authentication key will display as clear text. Refer to *service password-encryption on page 1699* for more information

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example specifies that the TACACS+ server at IP address **10.10.10.4** uses the global key setting (left unspecified), a timeout value of **10** seconds, and the default TCP port (left unspecified):

(config)**#tacacs-server host 10.10.10.4 timeout 10**

The following example specifies that the TACACS+ server at IP address **10.10.10.4** on VRF **RED**, uses the global key setting (left unspecified), a timeout value of **10** seconds, and the default TCP port (left unspecified):

(config)**#tacacs-server vrf RED host 10.10.10.4 timeout 10**

tcl run <*name*> track <*track name*>

Use the **tcl run track** command to initiate a tool command language (Tcl) script based on the result of monitoring the change of state of a track. Use the **no** form of this command to disable the track monitoring for the given script. This command is only available on platforms with Network Monitoring enabled. For more information on creating tracks, refer to *track <name> on page 1886* and the *Network Monitor Track Command Set on page 4098*. Variations of this command include:

tcl run <*name*> **track** <*track name*> **on-pass**
tcl run <*name*> **track** <*track name*> **on-fail**

Syntax Description

<*name*>	Specifies an inline Tcl script or Tcl script file.
<*track name*>	Specifies the name of the track to be monitored.
on-pass	Specifies the file should be run when the track meets the passing condition.
on-fail	Specifies the file should be run when the track meets the failure condition.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release R11.11.1	Command was expanded to include inline scripts.

Usage Examples

The following example activates a Tcl script to be run when the failure condition is met on **track_a**:

(config)**#tcl run test1.tcl track track_a on-fail**

tcl script *<name> <delimiter>*

Use the **tcl script** command to create a new named tool command language (Tcl) script, and enter the input mode for the new script.

Syntax Description

<name>	Specifies the name of the inline Tcl script to be created.
<delimiter>	Specifies the delimiter character to be used to terminate the input mode for the inline Tcl script.

Default Values

No default values are necessary for this command.

Command History

Release R11.11.1	Command was introduced.

Usage Examples

The following example creates the **test1** inline Tcl script, with **@** specified as the delimiter character, enters the input mode for the script, enters a Tcl command, and then exits the input mode using the specified delimeter character:

(config)**#tcl script test1 @**
e**vent notice “TEST”**
@
(config)**#**

telnet

Use the **telnet** command to open a Telnet session (through AOS) to another system on the network. Variations of this command include the following:

telnet <*ip address* | *hostname*>
telnet <*ip address* | *hostname*> **port** <*tcp port*>
telnet vrf <*name*> <*ip address* | *hostname*>
telnet vrf <*name*> <*ip address* | *hostname*> **port** <*tcp port*>

Syntax Description

<*ip address* | *hostname*>	Specifies the IP address or host name of the remote system. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
port <*tcp port*>	Optional. Specifies the Transmission Control Protocol (TCP) port number to be used when connecting to a host through Telnet. Range is **1** to **65535**.
vrf <*name*>	Optional. Specifies the virtual routing and forwarding (VRF) where the IP address or host name exists.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.
Release 14.1	Command was expanded to specify the port number.
Release 16.1	Command was expanded to include the **vrf** parameter.

Functional Notes

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the above mentioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example opens a Telnet session with a remote system (**10.200.4.15**):

>**enable**
#telnet 10.200.4.15
User Access Login:
Password:

The following example opens a Telnet session with a remote system (**10.200.4.15**) on port **8010**:

>**enable**
#telnet 10.200.4.15 port 8010
User Access Login:
Password:

telnet-server <*port*>

Use the **telnet-server** command to specify an alternate Transmission Control Protocol (TCP) port for Telnet servers. Use the **no** form of this command to return to the default setting.

Syntax Description

<*port*>	Specifies the alternate TCP port for the Telnet server.

Default Values

By default, the Telnet server listens on TCP port **23**.

Command History

Release 18.2	Command was introduced. This command replaces the **ip telnet-server** <*port*> command for Adtran internetworking products only.
Release R10.1.0	Command was introduced. This command replaces the **ip telnet-server** <*port*> command for Adtran voice products.

Usage Examples

The following example configures the Telnet server to listen on TCP port **2323**, instead of the default port **23**:

(config)**#ip telnet-server 2323**

To return to the default setting, use the **no** form of the command. For example:

(config)**#no telnet-server 2200**

test template match <*string*> to <*pattern*>

Use the **test template match to** command to evaluate dial strings and regular expressions for template matching and substitution. Once the command is entered, a response is provided indicating if the match was successful. Variations of this command include the following:

test template match <*string*> **to** <*pattern*>
test template match <*string*> **to** <*pattern*> **substitute-using** <*pattern*>

Syntax Description

<*string*>	Specifies a specific dial string to match. Valid entries can include a combination of characters ***** and **0** through **9**.
<*pattern*>	Specifies a pattern using either traditional number matching or regular expression matching methods. Refer to the *Functional Notes* below for more information.
substitute-using	Optional. Displays the resulting substitution.

Default Values

No default values are necessary for this command.

Command History

Release A4.05	Command was introduced.

Functional Notes

The <*pattern*> parameter can be defined using traditional number matching or regular expression matching methods. Traditional number matching uses numbers and wildcard variables to enter a pattern.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

In regular expressions number matching, the match strings are encapsulated by paired */* (slash) symbols. This indicates that the pattern is to be treated as a regular expression. Using regular expressions allows greater flexibility in matching multiple number templates with fewer expressions.

NOTE *AOS is compatible with Perl compatible regular expressions (PCREs). More information on understanding and using regular expressions is available at* http://www.pcre.org.

NOTE *The use of quotation marks in a command syntax, when entering a string is not necessary unless the string requires using a space or* **?***. Using either of these characters outside of quotation marks is interpreted by the command line interface (CLI) as a command and is not recognized as part of the string. The use of quotation marks in the following examples are provided to cover all possible user-entered strings. These examples can be entered without the quotation marks and function in the same manner.*

Usage Examples

The following is a sample response using the **test template match** command with traditional number matching:

(config)**#test template match “5551234” to “555XXXX”**
Match Result -> Match

The following is a sample response using the **test template match** command with regular expression matching:

(config)**#test template match “5551234” to “/555\d{4}/”**
Match Result -> Match

The following is a sample response using the **test template match** <*string*> **to** <*pattern*> **substitute-using** <*pattern*> command with traditional number matching:

(config)**#test template match “5551234” to “555XXXX” substitute-using “1359555XXXX”**
Substitute Result -> 13595551234

The following is a sample response using the **test template match** <*string*> **to** <*pattern*> **substitute-using** <*pattern*> command with regular expression matching:

(config)**#test template match “5552121DE” to “/(\d+).*/” substitute-using “/\1/”**
Substitute Result -> 5552121

tftp ip access-class <*ipv4 acl*> in

Use the **tftp ip access-class** class command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to all self-bound IPv4 Trivial File Transfer Protocol (TFTP) incoming connections. Use the **no** form of this command to remove the ACL. Variations of this command include:

tftp ip access-class <*ipv4 acl*> **in**
tftp ip access-class <*ipv4 acl*> **in any-vrf**
tftp ip access-class <*ipv4 acl*> **in vrf** <*name*>

Syntax Description

<*ipv4 acl*>	Specifies the IPv4 ACL to apply to the TFTP connections.
in	Specifies that the ACL is applied to incoming TFTP connections.
any-vrf	Optional. Allows incoming TFTP connections from any Virtual Routing and Forwarding (VRF) instance.
vrf <*name*>	Optional. Allows incoming TFTP connections from a specified VRF instance.

Default Values

By default, no ACLs are configured or applied to TFTP connections.

Command History

Release 18.2	Command was introduced.
Release R10.3.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example applies the previously configured IPv4 ACL **MatchAll** to inbound TFTP connections:

(config)**#tftp ip access-class MatchAll in**

tftp ipv6 access-class <*ipv6 acl*> in

Use the **tftp ipv6 access-class in** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to all self-bound IPv4 Trivial File Transfer Protocol (TFTP) incoming connections. Use the **no** form of this command to remove the ACL. Variations of this command include:

tftp ipv6 access-class <*ipv6 acl*> **in**
tftp ipv6 access-class <*ipv6 acl*> **in any-vrf**
tftp ipv6 access-class <*ipv6 acl*> **in vrf** <*name*>

Syntax Description

<*ipv6 acl*>	Specifies the IPv6 ACL to apply to the TFTP connections.
in	Specifies that the ACL is applied to incoming TFTP connections.
any-vrf	Optional. Allows incoming TFTP connections from any Virtual Routing and Forwarding (VRF) instance.
vrf <*name*>	Optional. Allows incoming TFTP connections from a specified VRF instance.

Default Values

By default, no ACLs are configured or applied to TFTP connections.

Command History

Release 18.2	Command was introduced.
Release R10.3.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example applies the previously configured IPv6 ACL **MatchAll** to inbound TFTP connections:

(config)**#tftp ipv6 access-class MatchAll in**

tftp server

Use the **tftp server** command to enable the Trivial File Transfer Protocol (TFTP) server. The **default-filesystem** parameter specifies the default location for the TFTP server to retrieve and store files. Use the **no** form of this command to disable the TFTP server. Variations of this command include:

tftp server
tftp server overwrite
tftp server default-filesystem cflash
tftp server default-filesystem flash
tftp server default-filesystem usbdrive0

Syntax Description

overwrite	Enables the TFTP server to overwrite existing files.
default-filesystem cflash	Optional. Specifies that the TFTP server use CompactFlash® as the default file system.
default-filesystem flash	Optional. Specifies that the TFTP server use flash as the default file system.
default-filesystem usbdrive0	Optional. Specifies that the TFTP server use Universal Serial Bus (USB) flash drive memory as the default file system.

Default Values

By default, this command is disabled.

Command History

Release 9.3	Command was introduced.
Release 13.1	Command was expanded to include the **overwrite** feature.
Release 17.3	Command was expanded to include the **default-filesystem** parameter.
Release 18.2	Command was changed from **ip tftp server** to **tftp server** to accommodate Internet Protocol version 6 (IPv6) for Adtran internetworking products only. In addition, the command was expanded to include the **usbdrive0** parameter.
Release R10.1.0	Command was changed from **ip tftp server** to **tftp server** to accommodate Internet Protocol version 6 (IPv6) for Adtran voice products.

Usage Examples

The following example enables the TFTP server:

(config)**#tftp server**

The following example specifies CompactFlash as the default file system:

(config)**#tftp server default-filesystem cflash**

tftp source-interface *<interface>*

Use the **tftp source-interface** command to use the specified interface's IP address as the source IP address for Trivial File Transfer Protocol (TFTP) client traffic transmitted by the unit. Use the **no** form of this command if you do not wish to override the normal source IP address.

Syntax Description

<interface>	Specifies the interface to be used as the source IP address for TFTP traffic. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **tftp source-interface ?** for a complete list of valid interfaces.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 14.1	Command was expanded to include the tunnel interface.
Release 17.1	Command was expanded to include the asynchronous transfer mode (ATM) interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release 18.2	Command was changed from **ip tftp source-interface** to **tftp source-interface** to incorporate Internet Protocol version 6 (IPv6) for Adtran internetworking products only.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.1.0	Command was changed from **ip tftp source-interface** to **tftp source-interface** to incorporate Internet Protocol version 6 (IPv6) for Adtran voice products.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for TFTP traffic:

(config)**#tftp source-interface loopback 1**

thresholds

Use the **thresholds** command to specify DS1 performance counter thresholds. Use the **no** form of this command to return to the default setting. Variations of this command include:

thresholds BES [15Min | 24Hr] <*number*>
thresholds CSS [15Min | 24Hr] <*number*>
thresholds DM [15Min | 24Hr] <*number*>
thresholds ES [15Min | 24Hr] <*number*>
thresholds LCV [15Min | 24Hr] <*number*>
thresholds LES [15Min | 24Hr] <*number*>
thresholds PCV [15Min | 24Hr] <*number*>
thresholds SEFS [15Min | 24Hr] <*number*>
thresholds SES [15Min | 24Hr] <*number*>
thresholds UAS [15Min | 24Hr] <*number*>

Threshold settings are applied to ALL DS1s.

Syntax Description

BES	Specifies the bursty errored seconds threshold.
CSS	Specifies the controlled slip seconds threshold.
DM	Specifies the degraded minutes threshold.
ES	Specifies the errored seconds threshold.
LCV	Specifies the line code violations threshold.
LES	Specifies the line errored seconds threshold.
PCV	Specifies the path coding violations threshold.
SEFS	Specifies the severely errored framing seconds threshold.
SES	Specifies the severely errored seconds threshold.
UAS	Specifies the unavailable seconds threshold.
15Min	Specifies that the threshold you are setting is for the counter's 15-minute statistics.
24Hr	Specifies that the threshold you are setting is for the counter's 24-hour statistics.
<*number*>	Specifies the maximum occurrences allowed for this error type. Once a threshold is exceeded, an event is sent to the console specifying the appropriate counter. Additionally, if Simple Network Management Protocol (SNMP) traps are enabled, the unit will send a trap with the same information as the console event.

Default Values

The default values for this command are as follows:

thresholds BES 15Min 10
thresholds BES 24Hr 100
thresholds CSS 15Min 1
thresholds CSS 24Hr 4
thresholds DM 15Min 1
thresholds DM 24Hr 4
thresholds ES 15Min 65
thresholds ES 24Hr 648
thresholds LCV 15Min 13340
thresholds LCV 24Hr 133400
thresholds LES 15Min 65
thresholds LES 24Hr 648
thresholds PCV 15Min 72
thresholds PCV 24Hr 691
thresholds SEFS 15Min 2
thresholds SEFS 24Hr 17
thresholds SES 15Min 10
thresholds SES 24Hr 100
thresholds UAS 15Min 10
thresholds UAS 24Hr 10

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the threshold for the 15-minute and 24-hour bursty errored seconds counter to **25** and **200**, respectively:

(config)**#thresholds BES 15Min 25**
(config)**#thresholds BES 24Hr 200**

timing-source

Use the **timing-source** command to configure the timing source used for reference timing. Use the **no** form of this command to return to the default setting. Variations of this command include the following:

timing-source e1 <*interface id*> **secondary**
timing-source e1 <*interface id*>
timing-source internal
timing-source internal secondary
timing-source t1 <*interface id*>
timing-source t1 <*interface id*> **secondary**

Syntax Description

e1 <*interface id*>	Recovers clocking from the specified E1 interface.
internal	Provides timing using the internal 1.544 MHz clock generator.
t1 <*interface id*>	Recovers clocking from the specified T1 or DSX-1 interface.
secondary	Optional. Signifies that the clock source specified in the command is to be the secondary clock source.

Default Values

By default, the primary clock source is set to **internal**.

Command History

Release 11.1	Command was introduced.
Release A5.01	Command was expanded to include the E1 interface.

Functional Notes

If both the primary and secondary clock sources fail, the unit automatically switches to internal timing.

Usage Examples

The following example configures the unit to use an internal timing source:

(config)**#timing-source internal**

The following examples set the t1 0/1 interface as the primary timing source and the t1 0/2 interface as the secondary timing source:

(config)**#timing-source t1 0/1**
(config)**#timing-source t1 0/2 secondary**

tls-profile *<profile name>*

Use the **tls-profile** command to enter the Transport Layer Security (TLS) Profile Configuration mode, from which the operation of TLS is configured. Use the **no** form of this command to remove the profile.

Syntax Description

<profile name>	Specifies the name of the TLS profile to create.

Default Values

By default, no TLS profiles exist.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Each entity on the AOS device that uses TLS must have a TLS profile applied in order to function. Many TLS profiles can exist and be referenced by many entities using TLS on the AOS device. The same TLS profile can be used by as many entities using TLS as required. The TLS profile essentially operates as a template for TLS operation and is applied on a per-trunk basis. For more information regarding TLS configuration, refer to the *SIP TLS Profile Command Set on page 4880*.

Usage Examples

The following example creates the TLS profile **TLSPROFILE1** and enters the profile's configuration mode:

```
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#
```


track *<name>*

Use the **track** command to create a track as part of network monitoring. This command is also used to enter into the Network Monitoring Track command set once a track is created. These additional commands are covered in *Network Monitor Track Command Set on page 4098*. Use the **no** form of this command to delete the track.

*Issuing the **shutdown** command once the track is configured will force the track to fail. Issuing the **no shutdown** command will enable the track.*

Syntax Description

<name>	Specifies the name of the track being created.

Default Values

By default, there are no tracks configured.

Command History

Release 13.1	Command was introduced.

Functional Notes

Track objects can be associated with probes to monitor their states. Upon a change in the probe state, the probe sends an event to any track registered with the probe. In response, the track performs the action indicated.

Track objects are associated with probes by using the commands *test if on page 4102* and *test list on page 4108*.

Usage Examples

The following example creates an track called **track_a**:

```
>enable
#configure terminal
(config)#track track_a
(config-track)#
```

Technology Review

Tracks are objects created to monitor other objects for a change in their state. The tracks can be configured to perform a specific action based upon the second object state detected. Association between a track and another object (for example, a probe, schedule, or interface) occurs through referencing the second object in the track's configuration. Once the track is registered with the second object, whenever a change occurs with that object's state, an event is sent to the track. Additional configuration commands are available for creating probes. These are explained in the *Network Monitor Probe Command Set on page 4062*.

username <*username*> password <*password*>

Use the **username password** command to configure the user name and password to use for all protocols requiring a user name-based authentication system, including File Transfer Protocol (FTP) server authentication, line (login local-user list), and Hypertext Transfer Protocol (HTTP) access. Using the **portal-list** parameter associates a portal list with the user. Using the **privilege** parameter specifies a privilege level for the user. Use the **no** form of this command to remove a user name and password. Variations of this command include:

username <*username*> **password** <*password*>
username <*username*> **portal-list** <*name*> **password** <*password*>
username <*username*> **portal-list** <*name*> **privilege** <*level*> **password** <*password*>
username <*username*> **privilege** <*level*> **password** <*password*>
username <*username*> **privilege** <*level*> **portal-list** <*name*> **password** <*password*>

Syntax Description

<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
password <*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive).
portal-list <*name*>	Optional. Specifies the name of the portal list assigned to this user.
privilege <*level*>	Optional. Specifies privilege level for this user. Valid entries are **1** to **7**.

Default Values

By default, there is no established user name or password. By default, there is no portal list assigned to user names. If this command is entered without a privilege level specified, the default privilege level assigned to the user is level 7.

Command History

Release 1.1	Command was introduced.
Release 17.1	Command was expanded to include the **portal-list** parameter.
Release A1	Command was expanded to include the **password** parameter.
Release R10.11.0	Command was expanded to include the **privilege** parameter.

Functional Notes

All users defined using the **username/password** command are valid for access to the unit using the **login local-userlist** command.

Before a portal list can be associated with a user name, it must be defined using the command *portal-list <name> <portal1 portal2 portal3> on page 1655*.

Usage Examples

The following example creates a user name of **Adtran** with password **Adtran**:

(config)**#username Adtran password Adtran**

The following example associates the portal list **ENGINEERS** with the user name **Adtran** and the password **Adtran**:

(config)**#username Adtran portal-list ENGINEERS password Adtran**

The following example specifies a privilege level **4** with the user name **Adtran** and the password **Adtran**:

(config)**#username Adtran privilege 4 password Adtran**

vlan *<vlan id>*

Use the **vlan** command to enter the Virtual Local Area Network (VLAN) Configuration mode. Use the **no** form of this command to remove a VLAN ID. Refer to the *VLAN Command Set on page 3356* for more information.

Syntax Description

<vlan id>	Specifies a valid VLAN ID. Range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enters the VLAN Configuration mode for VLAN 1:

```
(config)#vlan 1
(config-vlan 1)#
```


voice alias *<name>* equals *<number>*

Use the **voice alias equals** command to configure the name and number for the call routing alias. This feature allows a single call destination to be reached by an alternate name and number. Use the **no** form of this command to disable this feature.

Syntax Description

<name>	Specifies the alias name to describe the call destination.
<number>	Assigns the alias number to mask the original number.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example activates the **Lobby** voice alias at extension **4100**:

(config)**#voice alias Lobby equals 4100**

voice ani-list <*name*>

Use the **voice ani-list** command to create a list of automatic number identification (ANI) information and enter the ANI list configuration mode. Use the **no** form of this command to remove the ANI list.

Additional subcommands are available once you have entered the ANI list configuration mode:

ani <*template*>

Syntax Description

<*name*>	Specifies the name of the ANI list.
ani <*template*>	Specifies the ANI digits of the calling party to add to the ANI list. Digits include a combination of wildcards and numerical digits. Refer to the *Functional Notes* of this command for more information on using wildcards.

Default Values

By default, no ANI lists are configured.

Command History

Release A2	Command was introduced.

Functional Notes

ANI lists are used to permit or deny specific calling parties from accessing trunk groups to which the ANI list is applied.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example creates an ANI list called **TEST1** and specifies which numbers are included in the ANI list:

(config)**#voice ani-list TEST1**
(config-ani-list-TEST1)#ani 555-81xx

voice announcement trunk-unavailable

Use the **voice announcement trunk-unavailable** command to enable the playing of an announcement when a call is made and the trunk for that call is unavailable. Use the **no** form of this command to disable the option.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release R10.6.0	Command was introduced.

Usage Examples

The following example enables the trunk-unavailable announcement:

(config)**#voice announcement trunk-unavailable**

voice autoattendant

Use the **voice autoattendant** command to configure the auto attendant options for the system. Use the **no** form of the commands to disable the setting. For more voice auto attendant options, refer to *voice call-appearance-mode on page 1895*. Variations of this command include the following:

voice autoattendant <*name*>
voice autoattendant <*name*> **extension** <*number*>
voice autoattendant alias <*name*>
voice autoattendant did <*number*>
voice autoattendant extension <*number*>

Syntax Description

<*name*>	Specifies a name for this auto attendant.
alias <*name*>	Specifies an alias name to use as an alternate when accessing the auto attendant.
did <*number*>	Configures the direct inward dialing (DID) number to assign to the auto attendant.
extension <*number*>	Specifies the extension for auto attendant system login access.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example configures the **aOperator** as an alias for the auto attendant:

(config)**#voice autoattendant alias aOperator**

voice call-appearance-mode

Use the **voice call-appearance-mode** command to configure the unit to allow single or multiple call appearances to user account phones. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice call-appearance-mode multiple
voice call-appearance-mode single

Syntax Description

multiple	Allows multiple call appearances. For analog phones, this is limited to **2** call appearances; for Session Initiation Protocol (SIP) phones, **6** call appearances are allowed.
single	Allows only a single call appearance.

Default Values

By default, this is set to **multiple**.

Command History

Release 11.1	Command was introduced.

Functional Notes

Each incoming call is classified as a call appearance. For example, call waiting supports two call appearances simultaneously. Without call waiting, only one call appearance is supported at a time.

Usage Examples

The following example sets the unit to allow multiple call appearances:

(config)#**voice call-appearance-mode multiple**

voice caller-id timezone *<value>*

The **voice caller-id timezone** command sets the time zone used for the caller identification (ID) timestamp of an inbound call. This setting is independent of the clock timezone set by the command *clock timezone <value> on page 1234*. The caller ID timestamp is calculated using the system clock (*clock set <time> <day> <month> <year> on page 1233*) and the caller ID time zone offset. Use the **no** form of this command to disable this feature.

Syntax Description

<value>	Time zone values are specified in the *Functional Notes* section for this command.

Default Values

By default, the caller ID timezone is set to the current system time zone. For more information on the system time zone, refer to the command *clock timezone <value> on page 1234*.

Command History

Release R10.1.0	Command was introduced.

> NOTE *Depending on the **clock timezone** chosen, one-hour daylight savings time (DST) correction may be enabled automatically. Refer to the command clock on page 1232 for more information.*

Functional Notes

The following list shows sample cities and their time zone codes.

clock timezone +1-Amsterdam
clock timezone +1-Belgrade
clock timezone +1-Brussels
clock timezone +1-Sarajevo
clock timezone +1-West-Africa
clock timezone +10-Brisbane
clock timezone +10-Canberra
clock timezone +10-Guam
clock timezone +10-Hobart
clock timezone +10-Vladivostok
clock timezone +11
clock timezone +12-Auckland
clock timezone +12-Fiji
clock timezone +13
clock timezone +2-Athens
clock timezone +2-Bucharest
clock timezone +2-Cairo
clock timezone +2-Harare
clock timezone +8-Bejing
clock timezone +8-Irkutsk
clock timezone +8-Kuala-Lumpur
clock timezone +8-Perth
clock timezone +8-Taipei
clock timezone +9-Osaka
clock timezone +9-Seoul
clock timezone +9-Yakutsk
clock timezone +9:30-Adelaide
clock timezone +9:30-Darwin
clock timezone -1-Azores
clock timezone -1-Cape-Verde
clock timezone -10
clock timezone -11
clock timezone -12
clock timezone -2
clock timezone -3-Brasilia
clock timezone -3-Buenos-Aires

clock timezone +2-Helsinki
clock timezone +2-Jerusalem
clock timezone +3-Baghdad
clock timezone +3-Kuwait
clock timezone +3-Moscow
clock timezone +3-Nairobi
clock timezone +3:30
clock timezone +4-Abu-Dhabi
clock timezone +4-Baku
clock timezone +4:30
clock timezone +5-Ekaterinburg
clock timezone +5-Islamabad
clock timezone +5:30
clock timezone +5:45
clock timezone +6-Almaty
clock timezone +6-Astana
clock timezone +6-Sri-Jay
clock timezone +6:30
clock timezone +7-Bangkok
clock timezone +7-Kranoyarsk
clock timezone -3-Greenland
clock timezone -3:30
clock timezone -4-Atlantic-Time
clock timezone -4-Caracus
clock timezone -4-Santiago
clock timezone -5
clock timezone -5-Bogota
clock timezone -5-Eastern-Time
clock timezone -6-Central-America
clock timezone -6-Central-Time
clock timezone -6-Mexico-City
clock timezone -6-Saskatchewan
clock timezone -7-Arizona
clock timezone -7-Mountain-Time
clock timezone -8
clock timezone -9
clock timezone -0-Universal Coordinated Time (UTC)
clock timezone GMT-Casablanca
clock timezone GMT-Dublin

Usage Examples

The following example sets the caller ID time zone for Santiago, Chile.

>**enable**
(config)**#clock timezone -4-Santiago**

voice callerid-type *<method>*

Use the **voice callerid-type** command to specify the caller ID method for the system. Select the caller ID type that is required by your telecommunications provider. Use the **no** form of this command to disable the setting.

Syntax Description

<method>	Specifies the type of caller ID to use with the system. The available options are: • **Australia_FSK** • **Belgium_FSK** • **Canada_Stentor** • **Denmark_DTMF** • **Finland_DTMF** • **Italy_FSK** • **Mexico_FSK** • **Netherlands_DTMF** • **New Zealand_FSK** • **Norway_FSK** • **Sweden_DTMF** • **UK_BT** • **UK_CCA** • **United_Arab_Emirates_FSK** • **US_Bellcore**

Default Values

By default, the caller ID type is set to **US_Bellcore**.

Command History

Release 15.1	Command was introduced.
Release A2	Command was expanded to include **Australia_FSK**.
Release A4.05	Command was expanded to include **Mexico_FSK**.
Release A5.01	Command was expanded to include **United_Arab_Emirates_FSK**.
Release R14.2.0	Command was expanded to include **New Zealand_FSK**

Usage Examples

The following example specifies using the Italian method for the caller ID type:

(config)**#voice callerid-type Italy_FSK**

voice cause-code-map

Use the **voice cause-code-map** command to configure the cause code and Session Initiation Protocol (SIP) message numbers for the primary rate interface (PRI). Cause codes and SIP message numbers are associated with a particular connection failure, and notifies the system when problems occur. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice cause-code-map from-pri <*value*> <*value*>
voice cause-code-map to-pri <*value*> <*value*>

Syntax Description

from-pri <*value*> <*value*>	Enter the cause code number to map to the SIP message. The valid range is **1** to **127**. Next, enter the SIP message number to be used. The valid range is **400** to **606**.
to-pri <*value*> <*value*>	Enter the SIP message number to map to the PRI cause code map. The valid range is **400** to **606**. The second <*value*> is the PRI cause code number. The valid range is **1** to **127**.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example sets the cause code number to **28** to associate with SIP messages:

(config)**#voice cause-code-map from-pri 28**

voice class-of-service *<set name>*

Use the **voice class-of-service** command to create a voice class of service (CoS) rule set and to enter the Voice Class of Service command set. These additional commands are covered in *Voice CoS Command Set on page 4897*. Use the **no** form of this command to delete a configured CoS rule set.

Syntax Description

<set name>	Specifies the name of the CoS rule set.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates a new CoS rule set called **set1**:

```
(config)#voice class-of-service set1
Configuring New Level “set1”.
(config-cos-set1)#
```


voice codec-country <*name*>

Use the **voice codec-country** command to assign a country setting for the plain old telephone service (POTS) (analog) coder-decoders (CODECs). Use the **no** form of this command to delete a configured country setting.

Syntax Description

<*name*>	Specifies the CODEC country name. The available options are **Australia**, **Belgium**, **Canada**, **China_Hong_Kong**, **Denmark**, **Etsi**, **Finland**, **France**, **Germany**, **Ireland**, **Italy**, **Luxembourg**, **Mexico, Netherlands, New Zealand, Norway**, **Puerto_Rico**, **Spain**, **Sweden**, **Switzerland**, **United_Arab_Emirates**, **United_Kingdom**, and **United_States**.

Default Values

By default, the CODEC country setting is **United_States**.

Command History

Release 15.1	Command was introduced.
Release A2	Command was expanded to include **Australia**.
Release A2.04	Command was expanded to include **Belgium**, **France**, **Germany**, **Ireland**, **Italy**, **Luxembourg**, **Spain**, **Switzerland**, and **United_Kingdom**.
Release A4.05	Command was expanded to include **China_Hong_Kong**, **Denmark**, **Etsi**, **Finland**, **Mexico**, **Netherlands**, **Norway**, **Sweden**, and **United_Arab_Emirates**.
Release R14.2.0	Command expanded to include **New Zealand_FSK**

Usage Examples

The following example assigns **Canada** as the CODEC country:

(config)**#voice codec-country Canada**

voice codec-list <*name*>

Use the **voice codec-list** command to create a named coder-decoder (CODEC) list for call negotiation and to enter the CODEC list configuration mode. Use the **no** form of this command to delete a configured CODEC list.

Syntax Description

<*name*>	Specifies the CODEC list name.

Default Values

By default, there are no configured voice CODEC lists.

Command History

Release 9.3	Command was introduced.

Functional Notes

CODEC lists are list of CODECs arranged in preferred order with the first listed CODEC being the most preferred for call negotiation. Using the **voice codec-list** command enters the configuration mode for the CODEC list, where you can enter the types of CODECs to be used, and their order of preference. CODEC lists are then applied to interfaces, voice trunks, or voice accounts to be used for call negotiation. For more information on configuring and applying CODEC lists, refer to *Voice CODEC List Command Set on page 4893*.

Usage Examples

The following example creates a new CODEC list named **List1**:

```
(config)#voice codec-list List1
Configuring New Codec List “List1”.
(config-codec)#
```


voice codec-priority

Use the **voice codec-priority** command to specify which coder-decoder (CODEC) list is set as the priority. Use the **no** form of this command to disable the setting. Variations of this command include:

voice codec-priority trunk
voice codec-priority user
voice codec-priority offer-sdp

Syntax Description

trunk	Specifies using the trunk's CODEC list as the priority CODEC list.
user	Specifies using the user's CODEC list as the priority CODEC list.
offer-sdp	Specifies using Session Description Protocol (SDP) offer/answer exchanges to set CODEC priority.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release A2	Command was expanded to include the **offer-sdp** parameter.

Functional Notes

The **voice codec-priority** command specifies the CODEC selection method at the unit's global level. Selections are made from preconfigured CODEC lists. For more information about configuring and applying CODEC lists, refer to the *Voice CODEC List Command Set on page 4893*.

Usage Examples

The following example specifies using the trunk's CODEC list as the priority CODEC list:

(config)**#voice codec-priority trunk**

voice compand-type

Use the **voice compand-type** command to set the companding type to match your telecommunications provider. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice compand-type a-law
voice compand-type u-law

Syntax Description

a-law	Specifies the A-law compand type. This compand type is mainly used in European telephone networks for the conversion between analog and digital signals in pulse-code modulation (PCM) applications, and is similar to the North American U-law standard.
u-law	Specifies the U-law compand type.This compand type is also known as Mu-law, and is the PCM quasi-logarithmic curve. It is the 64 kbps standard North America voice amplitude sample used for encoding and decoding.

Default Values

By default, the companding type is set to **u-law**.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example configures the companding type to **a-law**:

(config)**#voice compand-type a-law**

voice conference local

Use the **voice conference local** command to configure the local conference feature. The **voice conferencing-mode** command must be first set to **local** before these commands will take effect. Refer to *voice conferencing-mode on page 1907*. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice conference local max-sessions <*number*>
voice conference local originator flashhook drop
voice conference local originator flashhook ignore
voice conference local originator flashhook split
voice conference local originator onhook persist
voice conference local originator onhook terminate
voice conference local party-disconnect continue
voice conference local party-disconnect transfer

Syntax Description

max-sessions <*number*>	Specifies the maximum number of simultaneous 3-way conference sessions. If set to 0, the maximum number of sessions is defined by the capability of the hardware platform.
originator	Specifies the behavior of actions performed by the conference originator once the conference has been established.
flashhook drop	Indicates that when a flashhook is issued, the last party added to the 3-way conference will be dropped and the call will continue between the two remaining parties.
flashhook ignore	Indicates that when a flashhook is issued, it will be ignored. The 3-way conference will continue without interruption.
flashhook split	Indicates that when a flashhook is issued, the 3-way conference will be split into two calls, one between the originator and the first party and one between the originator and the second party. When a flashhook is issued after the split, it will toggle the originator between the two calls.
onhook persist	Indicates that when the originator goes on-hook, the two parties in the conference are connected together.
onhook terminate	Indicates that when the originator goes on-hook, the remaining parties are disconnected.
party-disconnect	Specifies the conference behavior after a member disconnects.
continue	Indicates the conference is maintained with the remaining parties.
transfer	Indicates the conference is dropped and a direct connection between the remaining parties is re-established.

Default Values

By default, the **max-sessions** is set to **3**, **originator onhook** is set to **persist**, **originator flashhook** is set to **drop**, and **party-disconnect** is set to **continue**.

Command History

Release A2	Command was introduced.

Functional Notes

The voice conference local settings are only valid when the **voice conferencing-mode** is set to **local**. Refer to *voice conferencing-mode on page 1907* for more information.

Usage Examples

The following example sets the unit to a maximum of 5 local conference sessions:

(config)**#voice conference local max-sessions 5**

The following example sets the behavior of the conference session to ignore a flash-hook issued by the conference originator:

(config)**#voice conference local originator flashhook ignore**

voice conferencing-mode

Use the **voice conferencing-mode** command to determine if voice conferencing bridging will be handled within the unit or from a far-end conferencing server. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice conferencing-mode local
voice conferencing-mode network

Syntax Description

local	Specifies voice conferencing will be handled within the unit.
network	Specifies voice conferencing will be handled by a far-end conferencing server.

Default Values

By default, the voice conferencing mode is set to **network**.

Command History

Release A1	Command was introduced.

Functional Notes

The voice conferencing mode is only valid when the flashhook mode is set to **interpreted**. Refer to the command *voice flashhook mode on page 1921* for more information.

Usage Examples

The following example sets the conferencing mode to handle conference bridging within the local unit:

(config)**#voice conferencing-mode local**

voice country-code *<number>*

Use the **voice country-code** command to enter the country code for this location. The country code is used to determine if an incoming call is international. If a call originates from the Session Initiation Protocol (SIP) wide area network (WAN) and it matches the specified voice country code number, the call is not considered international and the country code is stripped before passing the call to the customer premises equipment (CPE). Use the **no** form of this command to delete the country code.

Syntax Description

<number>	Specifies the country code of this location. One, two, and three (maximum) digit country codes are accepted.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Functional Notes

For a comprehensive list of numeric country codes for specific countries, refer to the *International Configuration Guide* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies a **voice country-code** of **44** (United Kingdom):

(config)**#voice country-code 44**

voice coverage *<name>*

Use the **voice coverage** command to create and modify a global call coverage list to be used to control call routing when a user's phone is not answered. This command also enters the global call coverage configuration mode. Use the **no** form of this command to remove a call coverage list.

Syntax Description

<name>	Specifies a name for the call coverage list.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Functional Notes

The **voice coverage** command creates a global call coverage list for the AOS product and enters the list's configuration mode. The configurable options for this list are detailed in *Call Coverage Command Set on page 4718*.

The global call coverage list can be overridden on a per-user or per-group basis using the **coverage** command from the appropriate configuration mode.

Usage Examples

The following example specifies that the call coverage list named **Absent** be used for global call coverage:

```
(config)#voice coverage Absent
    Configuring New Global Call Handling List "Absent"
(config-gch)#
```


voice current-mode

Use the **voice current-mode** command to activate a particular system mode on the unit. Variations of this command include:

voice current-mode custom1
voice current-mode custom2
voice current-mode custom3
voice current-mode default
voice current-mode lunch
voice current-mode night
voice current-mode override
voice current-mode weekend

Syntax Description

[custom1-custom3]	Specifies the custom system mode to use.
default	Specifies using the default system mode.
lunch	Specifies using the lunch time system mode.
night	Specifies using the night time system mode.
override	Specifies using the override system mode.
weekend	Specifies using the weekend system mode.

Default Values

By default, the system mode is set to **default**.

Command History

Release A1	Command was introduced.

Functional Notes

This command is used to put the unit into a specific system mode. The unit remains in the activated system mode until it is changed manually or a schedule change occurs triggering a transition to another system mode. Schedules are configured using the command *voice system-mode on page 1971*.

If the system is in override, the unit will ignore any schedule that exists. The unit will stay in override until manually changed. This command is saved into the dynvoice-config file to preserve the state of the unit in case of power failure.

Usage Examples

The following example sets the current system mode to **lunch**:

(config)**#voice current-mode lunch**

voice dial-plan

Use the **voice dial-plan** command to add a global number complete pattern. Use the **no** form of this command to delete configured dial plans. Variations of this command include:

voice dial-plan <*pattern id*> **900-number** <*pattern*>
voice dial-plan <*pattern id*> **900-number** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **always-permitted** <*pattern*>
voice dial-plan <*pattern id*> **always-permitted** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **extensions** <*pattern*>
voice dial-plan <*pattern id*> **extensions** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **internal-operator** <*pattern*>
voice dial-plan <*pattern id*> **internal-operator** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **international** <*pattern*>
voice dial-plan <*pattern id*> **international** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **local** <*pattern*>
voice dial-plan <*pattern id*> **local** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **long-distance** <*pattern*>
voice dial-plan <*pattern id*> **long-distance** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **operator-assisted** <*pattern*>
voice dial-plan <*pattern id*> **operator-assisted** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **specify-carrier** <*pattern*>
voice dial-plan <*pattern id*> **specify-carrier** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **toll-free** <*pattern*>
voice dial-plan <*pattern id*> **toll-free** <*pattern*> **[**<*ndt name*>**| default | none]**
voice dial-plan <*pattern id*> **[user1 | user2 | user3]** <*pattern*>
voice dial-plan <*pattern id*> **[user1 | user2 | user3]** <*pattern*> **[**<*ndt name*>**| default | none]**

Syntax Description

<*pattern id*>	Specifies dial pattern identification. Valid range is **1** to **255**.
900-number	Adds a pattern to the 900 number group.
always-permitted	Adds a pattern to the always permitted group.
extensions	Adds a pattern to the internal group.
internal-operator	Adds a pattern to the internal operator group.
international	Adds a pattern to the international group.
local	Adds a pattern to the local group.
long-distance	Adds a pattern to the long distance group.
operator-assisted	Adds a pattern to the operator assisted group.
specify-carrier	Adds a pattern to the specify carrier group.
toll-free	Adds a pattern to the toll free group.
user1	Adds a pattern to the user 1 group.
user2	Adds a pattern to the user 2 group.
user3	Adds a pattern to the user 3 group.

<pattern>	Specifies a dialing pattern. You can enter a complete phone number, or wildcards can be used to define the dialing pattern. Refer to *Functional Notes* of this command for more information on using wildcards.
<ndt name>	Optional. Specifies the named-digit-timeout to associate with this dial plan entry. The named-digit-timeout is assigned a timeout value with the **voice timeouts named-digit-timeout** command (refer to *voice timeouts on page 1972*).
default	Optional. Sets the named-digit-timeout to the default value. The default value is set with the **voice timeouts interdigit** command (refer to *voice timeouts on page 1972*).
none	Optional. Indicates that no named-digit-timeout is associated with this dial plan entry.

Default Values

By default, no dial plans are configured.

Command History

Release 9.3	Command was introduced.
Release A2	Command was expanded to include the named-digit-timeouts.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example adds the pattern **8000** to the **local** group:

(config)**#voice dial-plan 1 local 8000**

The following example adds the pattern **NXX-XXXX** to the **local** group and associates it with the **short1** named-digit-timeout:

(config)**#voice dial-plan 2 local NXX-XXXX short1**

voice did <*number*> extension <*extension*>

Use the **voice did extension** command to add a direct inward dialing (DID) number. Use the **no** form of this command to delete a configured translation.

Syntax Description

<*number*>	Specifies the direct inward dial lookup number.
<*extension*>	Specifies the target account of the DID translation.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example directs DID number **5558123** to extension **8123**:

(config)**#voice did 5558123 extension 8123**

voice directory <*name*>

Use the **voice directory** command to create or modify a voice directory and enter the Voice Directory Configuration mode. Use the **no** form of this command to delete a configured voice directory. Variations of this command include:

voice directory <*name*>

The following additional subcommands are available once you have entered the Voice Directory Configuration mode:

directory-include <*number*> **first-name** <*name*>
directory-include <*number*> **first-name** <*name*> **last-name** <*name*>

Syntax Description

<*name*>	Specifies the name of the directory to create or modify.
directory-include <*number*>	Specifies the extension of the user to be added to the dial-by-name directory. Adding users to the directory allows them to call parties using a name stored in the system. Use the **no** form of this command to remove a user from the directory.
first-name <*name*>	Specifies the user's first name.
last-name <*name*>	Optional. Specifies the user's last name.

Default Values

By default, no voice directories are configured.

Command History

Release 14.1	Command was introduced.

Functional Notes

Adding a voice directory is useful when taking advantage of the dial-by-name feature. By default, a system directory is always available. All voice users are automatically added as members of the system directory.

Usage Examples

The following example creates a new **voice directory** with name **Engineering**:

(config)**#voice directory Engineering**

The following example adds **Jan Doe** to the **Engineering** dial-by-name directory:

(config)**#voice directory Engineering**
(config-dir)**#directory-include 5555 first-name Jan last-name Doe**

voice disconnect-mode

Use the **voice disconnect-mode** command to control the disconnect mode of the unit. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice disconnect-mode dialtone
voice disconnect-mode fast-busy

Syntax Description

dialtone	Specifies issuing dial tone after disconnect on the unit.
fast-busy	Specifies issuing fast-busy tone after disconnect on the unit.

Default Values

By default, this command is set to **dialtone**.

Command History

Release A2.03	Command was introduced.

Usage Examples

The following example configures the unit to disconnect issuing a **fast-busy** tone:

(config)**#voice disconnect-mode fast-busy**

voice emergency-services

Use the **voice emergency-services** command to enable the local emergency service numbers. Local emergency service numbers are configured automatically when the system country is specified. Use the **no** form of this command to disable the local emergency service numbers.

Syntax Description

No subcommands.

Default Values

By default, local emergency service numbers are enabled.

Command History

Release R10.3.0	Command was introduced.

Usage Examples

The following example disables local emergency service numbers:

(config)**#no voice emergency-services**

voice fax-tone

Use the **voice fax-tone** command to choose which tones initiate modem passthrough mode or T.38 mode. Use the **no** form of this command to inhibit a specified tone from initiating T.38 or modem passthrough call handling. Variations of this command include:

voice fax-tone default
voice fax-tone modem-passthrough default
voice fax-tone modem-passthrough t30-cng
voice fax-tone modem-passthrough v21-preamble
voice fax-tone modem-passthrough v25-ans
voice fax-tone modem-passthrough v25-ans-pr
voice fax-tone modem-passthrough v8-ansam
voice fax-tone modem-passthrough v8-ansam-pr
voice fax-tone t38 default
voice fax-tone t38 t30-cng
voice fax-tone t38 v21-preamble
voice fax-tone t38 v25-ans
voice fax-tone t38 v25-ans-pr
voice fax-tone t38 v8-ansam
voice fax-tone t38 v8-ansam-pr

Syntax Description

default	Restores the default tones for initiating modem passthrough mode or T.38 mode, depending on where it is used in the command syntax. For example, issuing **voice fax-tone default** restores defaults for both modes, while issuing **voice fax-tone t38 default** only restores defaults for T.38 mode.
modem-passthrough	Specifies modem passthrough mode.
t38	Specifies T.38 mode.
t30-cng	Specifies the T.30 calling tones.
v21-preamble	Specifies the V.21 preamble flag tones.
v25-ans	Specifies the V.25 answer tones.
v25-ans-pr	Specifies the V.25 answer tones with phase reversals.
v8-ansam	Specifies the V.8 answer tones with amplitude modulation.
v8-ansam-pr	Specifies the V.8 answer tones with amplitude modulation and phase reversals.

Default Values

By default, all tones are enabled for the **modem-passthrough** list. Only the **v21-preamble** is enabled by default for the T.38 list.

Command History

Release A2.04	Command was introduced.
Release A5.01	Command default was changed so that only the **v21-preamble** tone is enabled by default for the T.38 tone list.

Functional Notes

When a fax tone is enabled, the tone is eligible to initiate either modem-passthrough or T.38 handling, depending on the command entered. T.38 fax tone commands take priority over modem passthrough fax tone commands. For example, in the default configuration with all commands enabled, any detected tone on a call would cause a reINVITE to T.38, as long as T.38 is enabled on the user (or primary rate interface (PRI/CAS trunk). If T.38 is not enabled, the call would be reINVITED to G.711 in modem passthrough mode.

Usage Examples

The following example disables **t30-cng** fax tone for modem passthrough mode:

(config)**#no voice fax-tone modem-passthrough t30-cng**

voice feature-mode

Use the **voice feature-mode** command to configure control of the voice features. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice feature-mode local
voice feature-mode network

Syntax Description

local	Allows voice features to be handled by the local unit.
network	Allows voice features to be handled by the network.

Default Values

By default, the voice feature mode is set to **network**.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets the control of the voice features to the **local** unit:

(config)**#voice feature-mode local**

voice flashhook mode

Use the **voice flashhook mode** command to determine if flashhook events will be interpreted locally or will be forwarded to the far end. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice flashhook mode interpreted
voice flashhook mode transparent

Syntax Description

interpreted	Allows the local unit to interpret flashhook events.
transparent	Specifies flashhook events to be transparent to the provider.

Default Values

By default, the voice flashhook mode is set to **interpreted**.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets the flashhook mode to allow the local unit to interpret flashhook events:

(config)**#voice flashhook mode interpreted**

voice flashhook threshold *<min time> <max time>*

Use the **voice flashhook threshold** command to configure the minimum and maximum time the switch hook must be held to be interpreted as a flash. Use the **no** form of this command to return to the default setting.

Syntax Description

<min time>	Specifies minimum flashhook time in milliseconds. Valid range is from **300** to **1000** milliseconds.
<max time>	Specifies maximum flashhook time in milliseconds. Valid range is from **300** to **1000** milliseconds.

Default Values

By default, the flashhook threshold times are **300** milliseconds (minimum) and **1000** milliseconds (maximum).

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example configures the flashhook thresholds at a minimum of **400** to a maximum of **900**:

(config)**#voice flashhook threshold 400 900**

voice forward-mode

Use the **voice forward-mode** command to control the forwarding mode of the unit. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice forward-mode local
voice forward-mode network

Syntax Description

local	Allows forwards to be handled locally by the unit.
network	Allows forwards to be handled by the network.

Default Values

By default, this command is set to **network**.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example configures the unit to handle forwards locally:

(config)**#voice forward-mode local**

voice grouped-trunk *<name>*

Use the **voice grouped-trunk** command to create a grouped trunk and to enter the Grouped Trunk command set. Refer to *Voice Trunk Group Command Set on page 4704* for details. Use the **no** form of this command to delete a configured grouped trunk.

Syntax Description

<name>	Specifies the name of the trunk group.

Default Values

By default, there are no configured grouped trunks.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates the trunk group **trunk3**:

```
(config)#voice grouped-trunk trunk3
(config-TRUNK3)#
```

voice hold-reminder

Use the **voice hold-reminder** command to specify how long a call can be on hold before the hold reminder rings the phone again. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice hold-reminder <*value*>
voice hold-reminder <*value*> <*interval*>

Syntax Description

<*value*>	Specifies how long a call can be on hold before the hold reminder rings the phone again. Range is **5** to **30** seconds.
<*interval*>	Optional. Specifies the interval at which all subsequent reminder rings will occur. Range is **10** to **120** seconds.

Default Values

The defaults for this command are a **10**-second hold time before the first reminder ring with **30**-second intervals between subsequent rings.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the first reminder ring to occur after the call has been on hold for **20** seconds (with subsequent reminder rings occurring every **15** seconds until the call is picked up):

(config)**#voice hold-reminder 20 15**

voice international-prefix

Use the **voice international-prefix** command to configure the international prefix for this unit. Use the **no** form of this command to delete a configured prefix. Variations of this command include:

voice international-prefix <*prefix*>
voice international-prefix abbreviated

Syntax Description

abbreviated	Specifies the international prefix be replaced with a plus symbol (+) in the Session Initiation Protocol (SIP) header.
<*prefix*>	Specifies the up to four digits for the prefix.

Default Values

By default, there is no configured international prefix.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example configures **011** as the international prefix:

(config)**#voice international-prefix 011**

voice line *<name>*

Use the **voice line** command to create (or modify) a voice line and enter voice line's configuration mode. Use the **no** form of this command to delete a configured voice line.

Syntax Description

<name>	Specifies the name or description of the voice line.

Default Values

By default, there are no configured voice lines.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example creates the voice line **Public**, and enters its voice line configuration mode:

```
(config)#voice line Public
Configuring New Line “Public”.
(config-Public)#
```

voice logging smdr

Use the **voice logging smdr** command to enable local logging of station message detail records (SMDRs). Use the **no** form of this command to disable local logging of SMDR reporting.

Syntax Description

No subcommands.

Default Values

By default, SMDR reporting is disabled.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

SMDRs are used to log information about individual calls. The recorded information includes call timestamps, call lengths, participating parties, call origination and destination details, and other information related to calls made or received through the voice network system. Several programs are available that collect SMDR information in order to provide call accounting, find call trends, and supply network administrators with information about productivity. For more information about configuring SMDR in AOS, refer to the configuration guide *Configuring SMDR Reports for the NetVanta 7000 Series*, available online at https://supportofurms.adtran.com.

Usage Examples

The following example enables SMDR local logging:

(config)**#voice logging smdr**

voice logging smdr format

Use the **voice logging smdr format** command to specify the format of station message detail record (SMDR) logs. Use the **no** form of this command to return to the default SMDR format. Variations of this command include:

voice logging smdr format v1
voice logging smdr format v2

Syntax Description

v1	Specifies that SMDR version 1 is used.
v2	Specifies that SMDR version 2 is used.

Default Values

By default, **v1** SMDR formats are used.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

As of AOS firmware release R10.4.0, there are two SMDR versions. Both versions provide SMDRs in a single line of output that contains useful information about call activity. The first SMDR version (**v1**) provides the call date, time, duration, billing and origination codes, call originating and destination slot/port, calling and called party name and number, conference call flags, and special handling flags. The second SMDR version (**v2**) provides a unique ID for the call, the call date and start time, the call ring, hold, and billable time, the billing code, whether the call was internal or external, the originating and destination slot/port or trunk, calling and called party name and number, call destination name and ID, the dialed digits, the call status, and the SMDR version used to generate the call report. For more information about configuring SMDR in AOS, refer to the configuration guide *Configuring SMDR Reports for the NetVanta 7000 Series*, available online at https://supportofurms.adtran.com.

Usage Examples

The following example specifies that version 2 formatting is used for SMDR reporting:

(config)**#voice logging smdr format v2**

voice loopback *<number>*

Use the **voice loopback** command to configure the auto attendant options for the system. Use the **no** form of the commands to disable the setting. For more voice loopback account options, refer to *Voice Loopback Account Command Set on page 4546*.

Syntax Description

<number>	Specifies the extension for the loopback account.

Default Values

No default values are necessary for this command.

Command History

Release A1	Command was introduced.

Usage Examples

The following example creates a loopback with extension (account) number **5555**:

(config)**#voice loopback 5555**

voice mail

Use the **voice mail** command to configure voicemail options for the unit. Use the **no** form of this command to disable the setting. Refer to *voice mail check on page 1932* for additional arguments. Variations of this command include the following:

voice mail alias <*name*>
voice mail asterisk
voice mail class-of-service <*name*>
voice mail did <*number*>
voice mail extension <*extension*>
voice mail internal
voice mail leave-extension <*extension*>
voice mail max-login-attempts <*number*>

Syntax Description

alias <*name*>	Specifies an alias name to use as an alternate when accessing voicemail.
asterisk	Enables voicemail on an external Asterisk server.
class-of-service <*name*>	Configures the voicemail class of services.
did <*number*>	Configures the direct inward dialing (DID) number to assign to voicemail.
internal	Enables internal voicemail on the CompactFlash®.
extension <*extension*>	Specifies the extension users will dial to retrieve their voicemail.
leave-extension <*extension*>	Specifies the extension users will dial to leave a voicemail without ringing an extension. If a user forwards their phone to this extension, their calls will automatically forward to their voice mailbox.
max-login-attempts <*number*>	Specifies the maximum number login attempts to voicemail accounts. Range is **0** to **9** attempts.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command was expanded.

Usage Examples

The following example specifies extension **7500** for voicemail retrieval:

(config)**#voice mail extension 7500**

voice mail check

Use the **voice mail check** command to configure user parameters for the voicemail check extension. Use the **no** form of this command to disable the setting. Variations of this command include the following:

voice mail check alias <*name*>
voice mail check sip-identity <*station*> <*Txx*>
voice mail check sip-identity <*station*> <*Txx*> **register**
voice mail check sip-identity <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

alias <*name*>	Specifies an alias name to use as an alternate when accessing the check extension.
sip-identity <*station*> <*Txx*>	Specifies the station to be used for Session Initiation Protocol (SIP) trunk (e.g., **station extension**). Also, specifies the SIP trunk through which to register the server. The trunk is specified in the format Txx (e.g., **T01**).
register	Registers the user to the server.
auth-name <*username*>	Sets the user name that will be required as authentication for registration to the SIP server.
password <*password*>	Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example configures the **voice mail check sip-identity** to use extension **6000** as its identity on trunk **T04**:

(config)**#voice mail check sip-identity 6000 T04**

voice mail leave

Use the **voice mail leave** command to configure user parameters for the voicemail leave extension. Use the **no** form of this command to disable the setting. Variations of this command include the following:

voice mail leave alias <*name*>
voice mail leave sip-identity <*station*> <*Txx*>
voice mail leave sip-identity <*station*> <*Txx*> **register**
voice mail leave sip-identity <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

alias <*name*>	Specifies an alias name to use as an alternate when accessing the check extension.
sip-identity <*station*> <*Txx*>	Specifies the station to be used for Session Initiation Protocol (SIP) trunk (e.g., **station extension**). Also, specifies the SIP trunk through which to register the server. The trunk is specified in the format Txx (e.g., **T01**).
register	Registers the user to the server.
auth-name <*username*>	Sets the user name that will be required as authentication for registration to the SIP server.
password <*password*>	Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example configures the **voice mail leave sip-identity** to use extension **8000** as its identity on trunk **T06**:

(config)**#voice mail leave sip-identity 8000 T06**

voice mail sip-identity

Use the **voice mail sip-identity** command to configure Session Initiation Protocol (SIP) voicemail options for the unit. Use the **no** form of this command to disable the setting. Variations of this command include the following:

voice mail sip-identity <*sip ID*> <*sip trunk*>
voice mail sip-identity <*sip ID*> <*sip trunk*> **register**
voice mail sip-identity <*sip ID*> <*sip trunk*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

<*sip ID*> <*sip trunk*>	Specifies a number to be used as the SIP ID (e.g., **station extension**) and the SIP trunk through which you will register to the server.
register	Registers the user to the server.
auth-name <*username*>	Sets the user name that will be required as AUTHENTICATION for registration to the SIP server.
password <*password*>	Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command was expanded.

Usage Examples

The following example specifies trunk **T02** and extension **5800** for **voice mail sip-identity**:

(config)**#voice mail sip-identity 5800 T02**

voice match ani <*template*> substitute <*template*>

Use the **voice match ani substitute** command to configure automatic number identification (ANI) substitution for inbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

voice match ani <*template*> **substitute** <*template*>

Syntax Description

ani <*template*>	Specifies the ANI information to be substituted. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the ANI information that is substituted for the original ANI information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.

Default Values

By default, no ANI substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for ANI templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits

5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the ANI information from numbers **555-8111** to **555-8115** on all inbound trunks will be substituted by **555-8110**:

(config)**#voice match ani 555-811[1-5] substitute 555-8110**

Technology Review

The traditional ANI substitution feature operates at a global level on inbound trunks. The feature allows the substitution of calling party information with information determined by the user. This version of ANI substitution is applied only to internal caller ID at the inbound trunk, and only affects the number, not the name, of the calling party.

In this version of ANI substitution, DNIS substitution is also available. DNIS substitution is configured on a per-trunk basis for outbound trunks. DNIS substitution in this version only affects the number, not the name, of the called party.

voice mgcp-endpoint <*index*>

Use the **voice mgcp-endpoint** command to create a Media Gateway Control Protocol (MGCP) endpoint, assign it an index, and enter the endpoint configuration mode. Use the **no** form of this command to destroy the specified endpoint.

Syntax Description

<index>	Specifies the numerical value of the endpoint as part of the endpoint's default naming structure. Range is **1** to **255**.

Default Values

By default, no endpoints are configured.

Command History

Release A2	Command was introduced.

Functional Notes

By default, when endpoints are created and given an index number, they are named in the following format: **aaln/x**, where **x** is the index number. For example, an endpoint with an index of **4** will by default have the name **aaln/4**. The most common way of defining the index is to use the FXS port number, because the index is automatically appended to **aaln/** for the endpoint name.

Assigning an index is essential for creating an endpoint; however, endpoints can be renamed using the **name endpoint** command. Refer to *name <text> on page 4831* for more information.

Usage Examples

The following example creates an endpoint with an index of **1**, and enters the endpoint's configuration mode:

```
(config)#voice mgcp-endpoint 1
(config-mgcp-1)#
```


voice modem-passthrough-mode auto-disable-call-wait

Use the **voice modem-passthrough-mode auto-disable-call-wait** command to disable call waiting on fax and modem calls. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, automatic disabling of call waiting for fax/modem calls is disabled.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example disables call waiting on a fax call:

(config)**#voice modem-passthrough-mode auto-disable-call-wait**

voice music-on-hold mode

Use the **voice music-on-hold mode** command to configure the mode of the Music on Hold (MOH) feature. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice music-on-hold mode external
voice music-on-hold mode internal

Syntax Description

external	Specifies that on-hold music will play from a file stored locally on the unit.
internal	Specifies that on-hold music will play from an external device, such as an MP3 player or other device, plugged into the unit's MOH port.

Default Values

By default, this is set to **external**.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the MOH mode to **internal**:

(config)**#voice music-on-hold mode internal**

voice music-on-hold preferred-codec

Use the **voice music-on-hold preferred-codec** command to specify the coder-decoder (CODEC) format to use for the music on hold files. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice music-on-hold preferred-codec g711alaw
voice music-on-hold preferred-codec g711ulaw
voice music-on-hold preferred-codec g729

Syntax Description

g711alaw	Assigns the G.711 A-law CODEC (64000 bps) as the preferred CODEC for negotiation.
g711ulaw	Assigns the G.711 U-law CODEC (64000 bps) as the preferred CODEC for negotiation.
g729	Assigns the G.729 CODEC (8000 bps) as the preferred CODEC for negotiation.

Default Values

By default, the preferred CODEC is set to **g711ulaw**.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the preferred CODEC to **g711alaw**:

(config)**#voice music-on-hold preferred-codec g711alaw**

voice notify forward

Use the **voice notify forward** command to enable immediate call forwarding for analog voice users. This command causes the AOS device to play a certain stutter dial tone when the line is forwarded, alerting the subscriber that this line feature is enabled. Use the **no** form of this command to disable the feature. Variations of this command include:

voice notify forward disable-uri <*text*>
voice notify forward enable-uri <*text*>
voice notify forward parameter <*text*>

Syntax Description

disable-uri <*text*>	Specifies the Alert-Info uniform resource identifier (URI) that disables immediate call forwarding and produces the normal dialtone. When the disable URI is specified, the NOTIFY message is rejected and a 503 Service Unavailable response is generated. Specify the URI with a maximum of 256 characters.
enable-uri <*text*>	Specifies the Alert-Info URI that enables immediate call forwarding and produces the call forwarding dialtone. When the enable URI is specified, the NOTIFY message is accepted and a 200 OK response is generated. Specify the URI with a maximum of 256 characters.
parameter <*text*>	Specifies the Alert-Info parameter that indicates call forwarding is active. Specify the parameter with a maximum of 256 case-sensitive characters.

Default Values

By default, immediate call forwarding is disabled. When the feature is enabled, by default the normal and immediate call forwarding dial tones are set to an empty string, and the parameter value is set to an empty string.

Command History

Release R10.3.0	Command was introduced.

Functional Notes

The immediate call forwarding feature, when enabled, provides a specific dialtone which alerts the user that the feature is enabled. The specified dialtone occurs when the Alert-URI is matched in a NOTIFY message. For the feature to function, you must specify the Alert-URI that enables the feature and provides the feature dialtone (**enable-uri**), and you must specify the Alert-URI that disables the feature and provides the normal dialtone (**disable-uri**). If both parameters are not specified, the feature remains disabled.

This feature is available on all AOS voice platforms, and uses a country-specific dialtone when enabled. In all countries (excluding Mexico), the call forward indicator tone is equivalent to stutter-3. If both message waiting and call forwarding indication are enabled, stutter-3 is used for both features in all countries (excluding Mexico).

Usage Examples

The following example enables immediate call forwarding for analog users and specifies the normal and forwarding dial tones:

(config)**#voice notify forward enable-uri service:forward**
(config)**#voice notify forward disable-uri service:normal**

voice number-complete disable

Use the **voice number-complete disable** command to globally disable the default number-complete options. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice number-complete disable pound
voice number-complete disable star

Syntax Description

pound	Disables using the pound (#) key to indicate that a number is complete.
star	Disables using the star (*) key to indicate that a number is complete.

Default Values

By default, the pound (#) or star (*) key can be pressed to signify that the dialed number is complete.

Command History

Release A5.01	Command was introduced.

Functional Notes

When a user is dialing a phone number, the AOS unit will wait a configured amount of time (specified by the command *voice timeouts on page 1972*) after a digit is pressed before attempting to send the dialed set of digits. If the user does not want to wait for this timeout interval to elapse, the user can, by default, press either the pound (#) or star (*) key to indicate that the dialed number is complete.

Usage Examples

The following example disables using the pound (#) key to indicate that a number is complete:

(config)#**voice num-complete disable pound**

voice num-rings *<value>*

Use the **voice num-rings** command to globally specify the number of times a station will ring before beginning the coverage path that attempts to deliver a call to an available party. This setting can be overridden on a per-user basis using the **num-rings** command in the Voice User command set. Refer to *Voice User Account Command Set on page 4564* for more information. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the number of times a station can ring with no answer. Range is **0** to **9**. Setting to 0 allows unlimited rings.

Default Values

The default for this command is **0** (unlimited rings).

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets a limit on the number of times a station can ring:

(config)**#voice num-rings 8**

voice operator-group

Use the **voice operator-group** command to access the Voice Operator Group command mode. Refer to *Voice Operator Group Command Set on page 4664* for more information. Use the **no** form of this command to disable the setting.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example enters the Operator Group configuration mode:

```
(config)#voice operator-group
Configuring Operator Group.
(config-operator-group)#
```


voice overhead-paging connected-timeout <*value*>

Use the **voice overhead-paging connected-timeout** command to specify the timeout interval before an overhead paging call is terminated. Use the **no** form of this command to return to the default setting.

This setting does not affect calls placed into handset paging groups. It only affects calls to the overhead paging port on the back of the AOS unit.

Syntax Description

<*value*>	Specifies the timeout value in seconds. Set to **0** to disable the timeout.

Default Values

The default setting is **120** seconds.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example configures a connected timeout of **30** seconds for overhead paging:

(config)**#voice overhead-paging connected-timeout 30**

voice overhead-paging extension <*number*>

Use the **voice overhead-paging extension** command to specify the extension used for overhead paging. Use the **no** form of this command to disable the setting.

Syntax Description

<*number*>	Specifies the extension to use for overhead paging.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures extension **3000** to be used for overhead paging:

(config)**#voice overhead-paging extension 3000**

voice paging-group <*extension*>

Use the **voice paging-group** command to create a new handset paging group and enter the paging group's configuration. Use the **no** form of this command to remove the paging group.

Syntax Description

<*extension*>	Specifies the numeric extension for the paging group.

Default Values

By default, no paging groups exist.

Command History

Release A2.04	Command was introduced.

Functional Notes

The **voice paging-group** command enters the configuration for a handset paging group. For more information about handset paging, refer to the *Handset Paging for the NetVanta 7000 Series* quick configuration guide available online at https://supportcommunity.adtran.com.

For more information about the commands used to configure handset paging, refer to the *Voice Paging Group Command Set on page 4680*.

Usage Examples

The following example creates a paging group using extension **8956** and enters the group's configuration mode:

```
(config)#voice paging-group 8956
  Configuring new paging group "8956".
(config-8956)#
```


voice park-return <*value*>

Use the **voice park-return** command to configure the time until a parked call returns. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies time in seconds until a call returns from park if not retrieved. Valid range is **15** to **360** seconds.

Default Values

By default, the **voice park-return** time is set to **60** seconds.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets the time a call returns from park to **30** seconds:

(config)**#voice park-return 30**

voice pickup-group *<name>*

Use the **voice pickup-group** command to create a new call pickup group and enter the group's configuration mode.

Syntax Description

<name>	Specifies the name of the call pickup group.

Default Values

By default, no call pickup groups exist.

Command History

Release A4.01	Command was introduced.

Functional Notes

There is a limit of 10 call pickup groups on an AOS unit.

For more information about call pickup group configuration commands, refer to the *Voice Call Pickup Group Command Set on page 4653*.

For more information about configuring the call pickup feature, refer to the *Configuring the Call Pickup Feature on AOS Voice Products* quick configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the call pickup group **Sales** and enters the group's configuration mode:

```
(config)#voice pickup-group Sales
Configuring New Pickup Group "Sales"
(config-Sales)#
```


voice prompt-language <*language*>

Use the **voice prompt-language** command to specify the language to use for voice prompts (such as audios and voicemail menus) on the system. Use the **no** form of this command to disable the current language setting.

Syntax Description

<*language*>	Specifies the language to use for voice prompts. The available choices are **English** (American English), **FrenchCanadian, Irish** (Irish English), **LatinAmSpanish** (Latin American Spanish), and **UKEnglish** (United Kingdom English).

Default Values

The default value for this command is **English**.

Command History

Release 15.1	Command was introduced.
Release R10.2.0	The command was expanded to include the Irish language.

Usage Examples

The following example specifies the voice prompt language as Latin American Spanish:

(config)**#voice prompt-language LatinAMSpanish**

voice ring-group *<number>*

Use the **voice ring-group** command to create or modify ring group parameters. These additional commands are covered in *Voice Ring Group Command Set on page 4685*. Use the **no** form of this command to delete a configured ring group.

Syntax Description

<number>	Specifies the ring group's four-digit extension.

Default Values

By default, no ring groups are configured.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates a new ring group with extension **5678**:

(config)#**voice ring-group 5678**
Configuring New Group “5678”.
(config-5678)#

voice ring-option <*name*>

Use the **voice ring-option** command to create a ring option or modify an existing ring option. Once the ring option is configured, it can be applied to a shared line appearance (SLA) or shared call appearance (SCA). Use the **no** form of this command to delete a configured ring option. Additional subcommands are available once you have entered the Ring Option Configuration mode:

description <*text*>
ring-type delay-12-second
ring-type delay-24-second
ring-type immediate
ring-type silence
ring-type <*system mode*> **delay-12-second**
ring-type <*system mode*> **delay-24-second**
ring-type <*system mode*> **immediate**
ring-type <*system mode*> **silence**

Syntax Description

<*name*>	Specifies the name of the ring option. Limited to 10 characters.
description <*text*>	Optional. Provides a text description of the ring option. Limited to 40 characters.
ring-type <*system mode*>	Configures the ring behavior for the specified system mode. Not specifying a <*system mode*> implies changing the default system mode ring type. Enter one of the following to specify the system mode: **night**, **lunch**, **weekend**, **custom1**, **custom2**, **custom3**, or **override**. Enter a behavior to assign a ring type to the system mode:
immediate	Ring immediately.
silence	Visual ringing notification only.
delay-12-second	Ring after a 12 second delay.
delay-24-second	Ring after a 24 second delay.

Default Values

By default, the ring type is **immediate**.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example creates a new ring option named **SALES** and enters the Ring Option Configuration mode:

(config)**#voice ring-option SALES**
Configuring New Group “SALES”.
(config-SALES)**#**

The following example sets the ring type for the **weekend** system mode to **silence** for the **SALES** ring option:

(config-sales)**#ring-type weekend silence**

voice service map isdn-to-sip forward

Use the **voice service map isdn-to-sip forward** command to configure integrated services digital networking (ISDN) to Session Initiation Protocol (SIP) mappings for the call forwarding voice feature on the AOS unit. Variations of this command include:

voice service map isdn-to-sip forward busy disable-code <*spre code*>
voice service map isdn-to-sip forward busy enable-code <*spre code*>
voice service map isdn-to-sip forward no-response disable-code <*spre code*>
voice service map isdn-to-sip forward no-response enable-code <*spre code*>
voice service map isdn-to-sip forward unconditional disable-code <*spre code*>
voice service map isdn-to-sip forward unconditional enable-code <*spre code*>

Syntax Values

busy	Specifies the call forwarding busy special prefix (SPRE) code is configured and mapped.
no-response	Specifies the call forwarding no response SPRE code is configured and mapped.
unconditional	Specifies the call forwarding unconditional SPRE code is configured and mapped.
disable-code <*spre code*>	Disables the call forwarding feature for the specified SPRE code. Refer to *Functional Notes* for information about entering SPRE codes.
enable-code <*spre code*>	Enables the call forwarding feature for the specified SPRE code. Refer to *Functional Notes* for information about entering SPRE codes.

Default Values

By default, the call forwarding voice feature is not mapped between ISDN and SIP.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

The **voice service map isdn-to-sip forward** command does not have a **no** version. To disable mapping of a specific call forwarding feature, enter the **disable-code** parameter at the end of the command.

SPRE codes for this command are entered in the <**NX*> format, where **N** matches numbers from **2** to **9**, and **X** matches numbers from **0** to **9**. For example, ***25**. Display the currently assigned voice SPRE codes, using the *show voice spre* command.

Usage Examples

The following example enables ISDN to SIP mapping for the call forwarding busy feature on SPRE code **25**:

(config)**#voice service map isdn-to-sip forward busy enable-code *25**

The following example disables ISDN to SIP mapping for the call forwarding no response feature on SPRE code **30**:

(config)**#voice service map isdn-to-sip forward no-response disable-code *30**

voice service-mode

Use the **voice service-mode** command to add a service mode transition. Variations of this command include:

voice service-mode day <*day*> <*time*>
voice service-mode lunch <*day*> <*time*>
voice service-mode night <*day*> <*time*>
voice service-mode weekend <*day*> <*time*>

Syntax Description

day	Specifies a transition to day mode.
lunch	Specifies a transition to lunch mode.
night	Specifies a transition to night mode.
weekend	Specifies a transition to weekend mode.
<*day*>	Specifies the day of week the transition occurs.
<*time*>	Specifies the time for transition to occur (24-hour format - hours:minutes (HH:MM)).

Default Values

By default, the **voice service-mode** is set to **day**.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets the voice service mode to **day** with a transition day of Monday and a transition time of 8:00 AM:

(config)**#voice service-mode day monday 08:00**

voice speed-dial *<unique id> <number> <name>*

Use the **voice speed-dial** command to create a list of IDs to be used as shortcuts to contact frequently called numbers. Use the **no** form of this command to return to the default setting.

Syntax Description

<unique id>	The speed-dial number that will be used to contact the *<number>* specified.
<number>	Phone number associated with the speed-dial entry (digits only).
<name>	Description of this speed-dial entry.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets a speed-dial number of **8** for extension **9654**:

(config)**#voice speed-dial 8 9654 3rdFloorLab**

voice spre *<pattern id> <pattern>*

Use the **voice spre** command to add a global special prefix (SPRE) complete pattern. This command allows users to enter a custom SPRE code. Use the **no** form of this command to delete a configured SPRE pattern.

Syntax Description

<pattern id>	Specifies the SPRE pattern ID. Valid range is **1** to **255**.
<pattern>	Specifies the SPRE pattern. Refer to *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Functional Notes

This command allows users to enter a SPRE code pattern. Patterns begin with ***** or **#**. If the pattern is followed by an **&**, then the dial plan number-complete templates are used to determine when the unit has enough digits to dial the number (for example, **67&**). However, if a dial plan does not exist for a particular code that is needed, then a SPRE code may be entered followed by an independent dial plan number-complete template (for example, ***67NXX-XXXX**).

Valid characters for patterns are as follows:

0 - **9** Match the exact digit(s) only
X Match any single digit 0 through 9
N Match any single digit 2 through 9
M Match any single digit 1 through 8
& Allows the use of the dial-plan number complete pattern
[] Match any digit in the list within the brackets (for example, [1,4,6])
,() Formatting characters that are ignored but allowed
- Use within brackets to specify a range, otherwise ignored

The following are example pattern entries using wildcards:
EX1: *70&
EX2: #12NXXXXXX
EX3: *[1-3,9]0&

SPRE complete pattern rules:

1) The pattern must begin with ***** or **#**.
2) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
3) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
4) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
5) The **&** wildcard is only allowed at the end of the number.

Usage Examples

The following sets the complete pattern for SPRE 1:

(config)**#voice spre 1 *67NXX-XXXX**

voice spre-map

Use the **voice spre-map** command to change the default mapping of special prefix (SPRE) codes on the AOS voice product. Functions and SPRE codes can be disabled by using the **none** keyword. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice spre-map all none
voice spre-map auto-answer-dnd *<*nx*>
voice spre-map auto-answer-dnd none
voice spre-map billing-code *<*nx*>
voice spre-map billing-code none
voice spre-map block-callid-delivery *<*nx*>
voice spre-map block-callid-delivery none
voice spre-map call-forward-cancel *<*nx*>
voice spre-map call-forward-cancel none
voice spre-map call-forward-extension *<*nx*>
voice spre-map call-forward-extension none
voice spre-map call-forward-remote *<*nx*>
voice spre-map call-forward-remote none
voice spre-map call-held/park-retrieve *<*nx*>
voice spre-map call-held/park-retrieve none
voice spre-map call-park-zone *<*nx*>
voice spre-map call-park-zone none
voice spre-map call-return *<*nx*>
voice spre-map call-return none
voice spre-map call-user-speed-dial *<*nx*>
voice spre-map call-user-speed-dial none
voice spre-map camp-on *<*nx*>
voice spre-map camp-on none
voice spre-map cancel-camp-on *<*nx*>
voice spre-map cancel-camp-on none
voice spre-map clear-message-waiting *<*nx*>
voice spre-map clear-message-waiting none
voice spre-map conference *<*nx*>
voice spre-map conference none
voice spre-map cos-override *<*nx*>
voice spre-map cos-override none
voice spre-map disable-call-waiting *<*nx*>
voice spre-map disable-call-waiting none
voice spre-map dnd-enable-disable *<*nx*>
voice spre-map dnd-enable-disable none
voice spre-map door-phone *<*nx*>
voice spre-map door-phone none
voice spre-map door-unlock *<*nx*>
voice spre-map door-unlock none
voice spre-map fwd-notificatn-cancel *<*nx*>

voice spre-map fwd-notificatn-cancel none
voice spre-map group-login *<*nx*>
voice spre-map group-login none
voice spre-map group-logout *<*nx*>
voice spre-map group-logout none
voice spre-map hotel-login *<*nx*>
voice spre-map hotel-login none
voice spre-map hotel-logout *<*nx*>
voice spre-map hotel-logout none
voice spre-map maca-login *<*nx*>
voice spre-map maca-login none
voice spre-map maca-logout *<*nx*>
voice spre-map maca-logout none
voice spre-map page-overhead *<*nx*>
voice spre-map page-overhead none
voice spre-map permanent-hold *<*nx*>
voice spre-map permanent-hold none
voice spre-map program-speed-dial *<*nx*>
voice spre-map program-speed-dial none
voice spre-map redial *<*nx*>
voice spre-map redial none
voice spre-map remote-call-fwd-cancel *<*nx*>
voice spre-map remote-call-fwd-cancel none
voice spre-map send-to-vm *<*nx*>
voice spre-map send-to-vm none
voice spre-map set-account-password *<*nx*>
voice spre-map set-account-password none
voice spre-map set-message-waiting *<*nx*>
voice spre-map set-message-waiting none
voice spre-map system-mode *<*nx*>
voice spre-map system-mode none
voice spre-map system-speed-dial *<*nx*>
voice spre-map system-speed-dial none
voice spre-map transfer *<*nx*>
voice spre-map transfer none
voice spre-map user-station-lock *<*nx*>
voice spre-map user-station-lock none
voice spre-map user-station-unlock *<*nx*>
voice spre-map user-station-unlock none

*Not all SPRE codes are supported by all AOS products. Type **voice spre-map ?** to view a list of supported SPRE codes.*

Syntax Description

all	Makes the SPRE code assignment for all functions.
none	Removes the SPRE code for the specified function.
***<*nx*>**	Specifies the SPRE code to assign to this function. Valid range for *n* is **2** to **9**. Valid range for *x* is **0** to **9**.
auto-answer-dnd	Specifies the automatic answer do-not-disturb (DND) function.
billing-code	Specifies the billing code function.
block-callid-delivery	Specifies the block caller-ID delivery function.
call-forward-cancel	Specifies the call forward cancel function.
call-forward-extension	Specifies the call forward + extension function.
call-forward-remote	Specifies the call forward remote function.
call-held/park-retrieve	Specifies the held call pickup and park retrieve function
call-park-zone	Specifies the call park + zone function.
call-return	Specifies the call return function.
call-user-speed-dial	Specifies the call user speed dial function.
camp-on	Specifies the camp-on function.
cancel-camp-on	Specifies the cancel camp-on function.
clear-message-waiting	Specifies the clear message waiting function.
conference	Specifies the 3-way conferencing function.
cos-override	Specifies the class of service (CoS) override function.
disable-call-waiting	Specifies the disable call waiting on a per-call basis function.
dnd-enable-disable	Specifies the DND enable/disable function.
door-phone	Specifies the door phone function.
door-unlock	Specifies the door unlock function.
fwd-notificatn-cancel	Specifies the forward notification cancel function.
group-login	Specifies the group login function.
group-logout	Specifies the group logout function.
hotel-login	Specifies the hotel login function.
hotel-logout	Specifies the hotel logout function.
maca-login	Specifies the multiple access with collision avoidance (MACA) login function.
maca-logout	Specifies the MACA logout function.
page-overhead	Specifies the overhead paging function.
permanent-hold	Specifies the permanent hold function.
program-speed-dial	Specifies the program user speed dial function.
redial	Specifies the call last dialed number function.
remote-call-fwd-cancel	Specifies the remote call forward cancel function.
send-to-vm	Specifies the send directly to voicemail function.
set-account-password	Specifies the set account password function.

set-message-waiting Specifies the set message waiting function.
system-mode Specifies the system mode function.
system-speed-dial Specifies the system speed dial function.
transfer Specifies the transfer function.
user-station-lock Specifies the user station lock function.
user-station-unlock Specifies the user station unlock function.

Default Values

Default mappings between functions and SPRE codes are as indicated in the following table:

SPRE Code	Function	SPRE Code	Function
*21	Billing Code	*55	Group Login
*67	Block Caller ID Delivery	*56	Group Logout
*97	Auto-Answer Do-Not-Disturb	*78	Held Call Pickup/Call Park Retrieve
*35	Call Forward Cancel	*46	Hotel Login
*33	Call Forward + Extension	*47	Hotel Logout
*34	Call Forward Remote	*63	MACA Login
*77	Call Park + Zone	*64	MACA Logout
*69	Call Return	*30	Page Overhead
*62	Call User Speed Dial	*44	Permanent Hold
*66	Camp-on	*61	Program User Speed Dial
*65	Cancel Camp-on	*72	Redial
*86	Clear Message Waiting	*36	Remote Call Forward Cancel
*22	Conference 3-way	*79	Set Account Password
*90	Class of Service Override	*85	Set Message Waiting
*70	Disable Call Waiting Per Call Basis	*20	System Mode
*39	Do Not Disturb Enable/Disable	*25	System Speed Dial
*37	Door Phone	*88	Transfer
*38	Door Unlock	*57	User Station Lock
*32	Forward Notification Cancel	*58	User Station Unlock

Command History

Release A2.03 Command was introduced.

Release A5.01	Command was expanded to include the **page-intercom** parameter.
Release R10.2.0	Command was expanded to include the **send-to-vm** parameter.
Release R10.6.0	Command was expanded to include the **call-held/park-retrieve** parameter.
Release R11.5.0	Command was altered to remove the **page-intercom** parameter.

Functional Notes

SPRE codes are used to map a sequence of digits to a particular functionality. For example, in a typical network, *67 is used to block caller ID. The codes and their functions are listed in the Default Values. Functions and SPRE codes can be disabled by using the **none** keyword.

Usage Examples

The following example sets the SPRE code for call return to ***79**:

(config)**#voice spre-map call-return *79**

voice spre-mode

Use the **voice spre-mode** command to control whether special prefix (SPRE) codes will be interpreted by the unit locally or forwarded to the network for interpretation. The **override** parameter indicates that the specified SPRE code is to be overridden. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice spre-mode local
voice spre-mode network
voice spre-mode override *<*nx*>

Syntax Description

local	Specifies that SPRE codes are interpreted locally by the unit.
network	Specifies the forwarding of SPRE codes to the network for handling.
override *<*nx*>	Indicates the configured SPRE processing mode is overridden for the specified SPRE code. Valid range for *n* is **2** to **9**. Valid range for *x* is **0** to **9**.

Default Values

By default, this command is set to forward SPRE codes to the network and no overrides are configured.

Command History

Release 11.1	Command was introduced.
Release A2.03	Command was expanded to include the **override** option.

Functional Note

SPRE codes are used to map a sequence of digits to a particular functionality. For example, in a typical network, *67 is used to block caller ID. When the AOS unit is configured to operate in **network** mode, the digits are collected and sent to the network for appropriate handling. Using the **override** parameter allows the unit to be configured so that certain SPRE codes are collected locally and the corresponding function is initiated.

Usage Examples

The following example configures the unit to interpret SPRE codes:

(config)**#voice spre-mode local**

The following example configures the unit, which is configured to use the **network** mode, to instead interpret the SPRE code ***67** locally:

(config)**#voice spre-mode network**
(config)**#voice spre-mode override *67**

voice status-group

Use the **voice status-group** command to create or modify a voice status group and enter the Voice Status Group Configuration mode. Use the **no** form of this command to delete a voice status group. Variations of this command include:

voice status-group <*name*>

The following additional subcommands are available once you have entered the Voice Status Group Configuration mode:

park-zone <*value*>
user <*number*>
user <*number*> **display-name** <*name*>
user <*number*> **dial-string** <*string*>
user <*number*> **display-name** <*name*> **dial-string** <*string*>
use-spre-entities

Syntax Description

<*name*>	Specifies the name of the voice status group to create, modify, or delete.
park-zone <*value*>	Specifies a new park zone number to add to this voice status group. The valid range is **0** to **9**.
user <*number*>	Specifies the extension of a user to add to this voice status group.
display-name <*name*>	Optional. Specifies an override name to appear as the user's name when displayed on the device (BLF). If the name includes spaces, it must be surrounded by quotation marks as shown in the *Usage Examples*.
dial-string <*string*>	Optional. Specifies a specific number to dial. Valid entries can include a combination of characters ***** and **0** through **9**.
use-spre-entities	Specifies that the system use special prefix (SPRE) codes for extensible markup language (XML) entities in Notify messages when applicable.

Default Values

By default, there are no voice status groups configured.

Unless the user explicitly enters a **display-name** or **dial-string**, these values will default to the user's extension number. The **dial-string** and **display-name** cannot be added or changed after a user is added to a status group. The user must first be removed from the status group with the **no user** <*number*> command, then re-added as a member with the appropriate **display-name** and/or **dial-string**. Refer to the *Usage Examples* section for further details.

Command History

Release 14.1	Command was introduced.

Release A2	Command was expanded to include the dial string entries.
Release A5.01	Command was expanded to include the **use-spre-entities** parameter.

Usage Examples

The following example creates a new voice status group with the name **Engineering**:

(config)**#voice status-group Engineering**
The following example adds park zone **4** to the Engineering status group directory:

(config)**#voice status-group Engineering**
(config-status-Engineering)**#park-zone 4**

The following example adds user **5555** to the Engineering status group directory, displaying the default name **5555** with the default dial string of **5555**:

(config)**#voice status-group Engineering**
(config-status-Engineering)**#user 5555**

The following example adds user **5555** to the Engineering status group directory, displaying the name **Test Lab** with the default dial string of **5555**:

(config)**#voice status-group Engineering**
(config-status-Engineering)**#user 5555 display-name “Test Lab”**

The following example adds user **5555** to the Engineering status group directory, displaying the default name **5555** with a handsfree dial string of ****5555**:

(config)**#voice status-group Engineering**
(config-status-Engineering)**#user 5555 dial-string **5555**

The following example adds user **5555** to the Engineering status group directory, displaying the name **Test Lab** with a handsfree dial string of ****5555**:

(config)**#voice status-group Engineering**
(config-status-Engineering)**#user 5555 display-name “Test Lab” dial-string **5555**

voice status-group expires

Use the **voice status-group expires** command to add a status group subscription time for status group clients. Any subscription time requests that fall between the minimum and maximum values will be instructed to use the default value instead. Variations of this command include:

voice status-group default-expires <*value*>
voice status-group max-expires <*value*>
voice status-group min-expires <*value*>

Syntax Description

default-expires <*value*>	Specifies a default subscription time. The valid range is **120** to **86400** seconds.
max-expires <*value*>	Specifies a maximum subscription time. The valid range is **120** to **86400** seconds.
min-expires <*value*>	Specifies a minimum subscription time. The valid range is **120** to **86400** seconds.

Default Values

By default, the voice status group **default-expires** value is set to **120** seconds, **max-expires** value is set to **3600**, and the **min-expires** is set to **86400**.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example sets the voice status group maximum subscription time to 2 hours:

(config)**#voice status-group max-expires 7200**

voice system-country *<name>*

Use the **voice system-country** command to specify the system country setting. Specifying the system country with this command automatically changes several default settings to match the standards of the specified country. Refer to the *Functional Notes* for details. Use the **no** form of this command to return to the default setting.

Syntax Description

<name>	Specifies the system country name. The available options are: **Australia**, **Belgium**, **Canada**, **China_Hong_Kong**, **Denmark**, **ETSI**, **Finland**, **France**, **Germany**, **Ireland**, **Italy**, **Luxembourg**, **Mexico**, **Netherlands**, **New Zealand**, **Norway**, **Puerto_Rico**, **Spain**, **Sweden**, **Switzerland**, **United_Arab_Emirates**, **United_Kingdom**, and **United_States**.

Default Values

The default system country code is **United_States**.

Command History

Release A2.04	Command was introduced.
Release A4.05	Command was modified to accept the country name instead of numbers.
Release R14.2.0	Command was expanded to include New **Zealand_FSK**

Functional Notes

The **voice system-country** command automatically sets the parameters for multiple settings on the AOS device to match the standards of the specified country. For example, Web-based graphical user interface (GUI) language, voice prompt language (if applicable), call progress tones, commanding type, caller ID type, and voice country code. The values for these parameters can be viewed using *show system on page 1036*.

The system country setting is not stored as part of the running configuration or startup configuration. Erasing the startup configuration will not change the system country. If a particular feature or configuration option is set to something other than the default, changing the system country will not effect that feature or option. For a comprehensive list of the features affected by the system country setting, refer to the *International Configuration Guide* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example sets the system country to **Canada**:

(config)**#voice system-country Canada**

voice system-mode

Use the **voice system-mode** command to configure the system mode schedules. When triggered by the system-clock, AOS units transition into a system mode based on the schedule. Use the **no** form of this command to disable the setting. Variations of this command include the following:

voice system-mode custom1 *<day> <time>*
voice system-mode custom2 *<day> <time>*
voice system-mode custom3 *<day> <time>*
voice system-mode default *<day> <time>*
voice system-mode lunch *<day> <time>*
voice system-mode night *<day> <time>*
voice system-mode weekend *<day> <time>*

Syntax Description

<day>	Specifies the day of the week. Choose from Sunday through Saturday.
<time>	Specifies the time of the day in a 24-hour format hours:minutes (HH:MM).
custom1 - custom3	Indicates the custom mode (1 through 3) to configure.
default	Indicates the default-time system mode to configure.
lunch	Indicates the lunch-time system mode to configure.
night	Indicates the night-time system mode to configure.
weekend	Indicates the weekend system mode to configure.

Default Values

By default, no system mode commands are configured, the unit will operate in the **default** mode.

Command History

Release A1	Command was introduced.

Usage Examples

The following example configures a typical 5-day business week:

(config)**#voice system-mode default Monday 8:00**
(config)**#voice system-mode night Monday 17:00**
(config)**#voice system-mode default Tuesday 8:00**
(config)**#voice system-mode night Tuesday 17:00**
(config)**#voice system-mode default Wednesday 8:00**
(config)**#voice system-mode night Wednesday 17:00**
(config)**#voice system-mode default Thursday 8:00**
(config)**#voice system-mode night Thursday 17:00**
(config)**#voice system-mode default Friday 8:00**
(config)**#voice system-mode weekend Friday 17:00**

voice timeouts

Use the **voice timeouts** command to configure the time limits for phases. Use the **no** form of this command to return to the default setting or remove the named digit timeout (NDT) and its value.

When removing an NDT and its value, if the NDT is assigned to a dial plan entry, then the deletion is not allowed. The dial plan must be removed first and added back into the system without the NDT association.

Variations of this command include:

voice timeouts alerting <*value*>
voice timeouts connected <*value*>
voice timeouts connecting <*value*>
voice timeouts emergency-callback <*value*>
voice timeouts interdigit <*value*>
voice timeouts named-digit-timeout <*ndt name*>
voice timeouts named-digit-timeout <*ndt name*> <*value*>
voice timeouts preconnected <*value*>
voice timeouts preconnecting <*value*>

Syntax Description

alerting <*value*>	Specifies the maximum time a call is allowed to remain in the alerting state. The shorter of this timeout or the configured maximum number of rings will determine how long a call is allowed to ring. The valid range is **0** (unlimited) to **60** minutes.
connected <*value*>	Specifies the maximum time a call is allowed to remain in the connected state. The valid range is **0** (unlimited) to **1000** hours.
connecting <*value*>	Specifies the maximum time a call is allowed to remain in the connecting state. The valid range is **0** (unlimited) to **60** minutes.
emergency-callback <*value*>	Specifies the maximum time to wait for an emergency callback. The valid range is **0** to **300** seconds.
interdigit <*value*>	Specifies the maximum time allowed between dialed digits. The valid range is **1** to **16** seconds.
named-digit-timeout	Creates a timeout with a name and a value to associate with a dial plan template.
<*ndt name*>	Specifies the name of the named-digit-timeout to be created.
<*value*>	Optional. Indicates the timeout value in seconds to allow after the last digit is dialed before routing the call. The valid range is **1** to **16** seconds.
preconnected <*value*>	Specifies the maximum time a call is allowed to stay in a preconnected state. The valid range is **0** (unlimited) to **60** minutes.
preconnecting <*value*>	Specifies the maximum time a call is allowed to stay in a preconnecting state. The valid range is **0** (unlimited) to **60** minutes.

Default Values

By default, the **alerting** timeout is 5 minutes, the **connected** timeout is 12 hours, and the **interdigit** timeout is 4 seconds. If no value is indicated for the NDT, 0 seconds is applied.

Command History

Release 14.1	Command was introduced.
Release A2	Command was expanded to include the **named-digit-timeouts** parameter.
Release R10.4.0	Command was expanded to include the **connecting**, **emergency-callback**, **preconnected**, and **preconnecting** parameters.

Functional Notes

The **named-digit-timeout** parameter allows multiple interdigit timeouts within the system. It provides a means for associating a specific amount of time to wait after a template match is made before routing a call. This added functionality allows short numbers and long numbers to coexist in the same system (for example, seven- and ten-digit patterns) without specifying additional characters (such as 1 or 9).

Usage Examples

The following example sets the alerting timeout to **30** seconds:

(config)**#voice timeouts alerting 30**

The following example creates a named-digit-timeout named **short1** and sets the timeout value to **2** seconds:

(config)**#voice timeouts named-digit-timeout short1 2**

voice transfer

Use the **voice transfer** command to set the unattended transfer for the system only. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice transfer blind
voice transfer unattended

Syntax Description

blind	Converts unattended transfer attempts to RFC 3891-compliant blind transfers.
unattended	Unattended transfer attempts are not modified.

Default Values

The default setting is **unattended**.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example configures the **voice transfer** type to **blind**:

(config)**#voice transfer blind**

voice transfer-mode

Use the **voice transfer-mode** command to specify whether transferred calls will be controlled by the unit locally, or if the network will control them. Use the **no** form of this command to return to the default setting. Variations of this command include:

voice transfer-mode local
voice transfer-mode network

Syntax Description

local	Specifies that call transferring is controlled locally by the unit.
network	Specifies that call transferring is controlled by the network.

Default Values

By default, the network controls call transfers.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the unit to handle call transfers:

(config)**#voice transfer-mode local**

voice transfer-on-hangup

Use the **voice transfer-on-hangup** command to enable this feature. When transferring a call, hanging up initiates the transfer to the destination party. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is enabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables this feature:

(config)**#voice transfer-on-hangup**

voice trunk access-code

Use the **voice trunk access-code** command to modify the outbound trunk access code. Use the **no** form of this command to remove the trunk access code and return to the default. Variations of this command include:

voice trunk access-code <*number*>
voice trunk access-code none

Syntax Description

<*number*>	Specifies the digit to use as the outbound trunk access code. Valid entries are **0** through **9**.
none	Specifies that no trunk access code is required to place outbound calls.

Default Values

By default, the outbound trunk access code is **9**.

Command History

Release R10.8.0	Command was introduced.

Functional Notes

There are a number of considerations involved if the trunk access code is changed or omitted on a previously installed system using the **voice trunk access-code** command. The following items should be reviewed to confirm that the correct steering digit is configured in each of these areas of AOS:

- User account call forwarding
- External call coverage for user accounts, ring groups, operator groups, and globally
- User account FindMe-FollowMe refer actions
- SIP trunk account outbound match ANI Add/Replace Diversion/P-Asserted-Identity commands
- ISDN/SIP trunk account, outbound match ANI substitute commands
- ISDN/SIP/Analog trunk account, outbound match DNIS substitute/replace ani commands
- Shared line account, external call coverage
- Shared call appearance, external call coverage
- Voicemail session: returning a call to the sender of a message
- Auto attendant, transfers to external numbers
- Recording and playing audio prompts from an external number
- Auto attendant, dial-by-name directory entries
- Status group member, external dial strings
- Class of service, advanced permit/deny templates
- System dial plan templates
- Global inbound match ANI substitution

Usage Examples

The following example configures the outbound trunk access-code as **7**:

(config)**#voice trunk access-code 7**

voice trunk-list <*name*>

Use the **voice trunk-list** command to create a permit/deny trunk list and to enter the trunk list configuration mode. Use the **no** form of this command to remove the trunk list.

Additional subcommands are available once you have entered the trunk list configuration mode:

trunk <*Txx*>

Syntax Description

<*name*>	Specifies the name of the trunk list.
trunk <*Txx*>	Specifies the trunk to add to the trunk list. Trunks are specified by their 2-digit identifier. For example, **T01**.

Default Values

By default, no trunk lists are configured.

Command History

Release A2	Command was introduced.

Functional Notes

The trunk lists are permit/deny lists that operate in the same manner as automatic number identification (ANI) lists, and are used to specify trunks that will be permitted or denied access on specified voice trunk groups.

There is no limit on the number of trunks that can be added to the trunk list, and there is no limit on the number of trunk lists that can be applied to a voice trunk group. The trunk lists are applied to the trunk group in the order they are listed.

Although there is no limit on the number of trunks allowed in a trunk list, or the number of trunk lists applied to voice trunk groups, it is important to remember that the more lists that are applied to a trunk group, the more the runtime performance of call routing will be affected.

Usage Examples

The following example creates a trunk list called **TEST2** and specifies the trunks to be included in the list:

(config)**#voice trunk-list TEST2**
(config-trunk-list-TEST2)**#trunk T01**
(config-trunk-list-TEST2)**#trunk T03**

voice trunk <*trunk id*> type

Use the **voice trunk type** command to define a new trunk for use with a Session Initiation Protocol (SIP) or integrated services digital network (ISDN) interface. Executing this command activates the Voice Trunk Configuration mode for the individual trunk. Refer to *Voice ISDN Trunk Command Set on page 5008* for information on the commands in that mode. Other trunk types are explained in *voice trunk <trunk id> type analog supervision on page 1981*. Use the **no** form of this command to delete a configured voice trunk. Variations of this command include:

voice trunk <*trunk id*> **type isdn**
voice trunk <*trunk id*> **type sip**

Refer to the configuration guide Voice Traffic over SIP Trunks and Configuring the Total Access 900 Series PRI Interface guide for more information on voice trunks. These documents are available online at http://supportforums.adtran.com.

Syntax Description

<*trunk id*>	Specifies the trunk's two-digit identifier in the format Txx (for example, **T12**).
isdn	Configures the trunk for use with ISDN service.
sip	Configures this trunk for use with SIP.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the analog and ISDN support.

Usage Examples

The following example creates the new trunk T12 for use with SIP and enters the Voice Trunk Configuration mode:

(config)**#voice trunk t12 type sip**
(config-T12)#

voice trunk *<trunk id>* type analog supervision

Use the **voice trunk type analog supervision** command to define a new trunk for an analog interface. Executing this command activates the Voice Trunk Analog Configuration mode for the individual trunk. Use the **no** form of this command to delete a configured voice trunk. Refer to *Voice Analog Trunk Command Set on page 4959* for information on the commands in that mode. Variations of this command include the following:

voice trunk *<trunk id>* **type analog supervision dpt**
voice trunk *<trunk id>* **type analog supervision ground-start**
voice trunk *<trunk id>* **type analog supervision loop-start**

Syntax Description

<trunk id>	Specifies the trunk's two-digit identifier in the format Txx (for example, **T01**).
dpt	Specifies dial pulse terminate (DPT) with an assumed user role.
ground-start	Specifies ground start (GS) with an assumed user role.
loop-start	Specifies loop start (LS) with an assumed user role.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example creates the new trunk **T15** for use with an analog interface and enters the Voice Trunk Analog DPT Configuration mode:

(config)**#voice trunk t15 type analog supervision dpt**
(config-T15)#

voice trunk *<trunk id>* type t1-rbs supervision

Use the **voice trunk type t1-rbs supervision** command to define a new trunk for a T1 interface. Executing this command activates the Voice Trunk T1 Configuration mode for the individual trunk. Use the **no** form of this command to delete a configured voice trunk. Refer to *Voice T1 Trunk Command Set on page 5151* for information on the commands in that mode. Other trunk types are explained in *voice trunk <trunk id> type on page 1980*. Variations of this command include the following:

voice trunk *<trunk id>*
voice trunk *<trunk id>* **type t1-rbs supervision fgd role user**
voice trunk *<trunk id>* **type t1-rbs supervision ground-start role user**
voice trunk *<trunk id>* **type t1-rbs supervision immediate role network**
voice trunk *<trunk id>* **type t1-rbs supervision immediate role user**
voice trunk *<trunk id>* **type t1-rbs supervision loop-start role user**
voice trunk *<trunk id>* **type t1-rbs supervision tie-fgd**
voice trunk *<trunk id>* **type t1-rbs supervision wink role network**
voice trunk *<trunk id>* **type t1-rbs supervision wink role user**

Syntax Description

<trunk id>	Specifies the trunk's two-digit identifier in the format Txx (for example, **T01**).
fgd	Specifies feature group D (FGD) with an assumed user role.
ground-start	Specifies ground start (GS) with an assumed user role.
immediate	Specifies E&M immediate with an assumed network or user role.
loop-start	Specifies loop start (LS) with an assumed user role.
tie-fgd	Specifies tie trunk with FGD.
wink	Specifies wink with an assumed network or user role.
role network	Specifies the network role for this trunk.
role user	Specifies the user role for this trunk.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 12.1	Command was expanded.

Usage Examples

The following example creates the new trunk **T15** for use with a T1 interface and enters the Voice Trunk T1 Wink Configuration mode:

```
(config)#voice trunk t15 type t1-rbs supervision wink role network
(config-T15)#
```


voice user <*extension*>

Use the **voice user** command to create a new user extension and to enter the Voice User command set. Use the **no** form of this command to delete a configured extension or modify an existing extension's parameters. Refer to *Voice User Account Command Set on page 4564* for details.

Syntax Description

<*extension*>	Specifies user's extension.

Default Values

By default, there are no configured voice users.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates a new user with extension **9876**:

(config)#**voice user 9876**
Configuring New User "9876".
(config-9876)#

voip name-service host

Use the **voip name-service host** command to add a host to the Voice over Internet Protocol (VoIP) name service (VNS) cache table. Using the **no** form of this command removes the host from the cache. Variations of this command include:

voip name-service host <*hostname*> **mgcp**
voip name-service host <*hostname*> **mgcp tcp**
voip name-service host <*hostname*> **mgcp udp**
voip name-service host <*hostname*> **sip**
voip name-service host <*hostname*> **sip tcp**
voip name-service host <*hostname*> **sip tls**
voip name-service host <*hostname*> **sip tls srv** <*service-name-prefix*>
voip name-service host <*hostname*> **sip tls srv** <*service-name-prefix*> <*transport-name-prefix*>
voip name-service host <*hostname*> **sip udp**

Syntax Description

<*hostname*>	Specifies the fully qualified domain name (FQDN) of the added host.
mgcp	Specifies that Media Gateway Control Protocol (MGCP) is the service type for the VNS service request.
sip	Specifies that Session Initiation Protocol (SIP) is the service type for the VNS service request.
tcp	Optional. Specifies that Transmission Control Protocol (TCP) is the protocol used for the service request.
tls	Optional. Specifies that Transport Layer Security (TLS) is the protocol used for the service request.
srv	Optional. Specifies that service records (SRV) parameters are enabled. Available only when an FQDN has been specified.
<*service-name-prefix*>	Optional. Specifies the service name prefix for the domain naming system (DNS) service (SRV) request. Underscores are added automatically.
<*transport-name-prefix*>	Optional. Specifies the transport prefix for the DNS SRV request. Underscores are added automatically.
udp	Optional. Specifies that User Datagram Protocol (UDP) is the protocol used for the service request.

Default Values

By default, both MGCP and SIP VNS requests use UDP. By default, SIP TLS requests use **SIPS** as the service name prefix and **TCP** as the transport name prefix.

Functional Notes

Voice and media signaling protocols (such as SIP) often rely on DNS

in order to ease configuration and administration of endpoints and also to implement redundancy mechanisms provided by DNS service records. Because voice and media signaling protocols are often directly coupled to a user experience, applications are often very sensitive to latency introduced by the DNS mechanism.

AOS voice products rely on the ability to resolve names to one or more service or address records quickly in order to place a call or register to an external voice server. The DNS server is often not local to the AOS unit, and it is not guaranteed to be accessible, even when other mechanisms necessary for successful call completion may be available. A DNS request for a particular host name results in local caching by the AOS unit, after which the DNS information is quickly available without requiring additional requests. The cache remains populated until the cached record expires.

The VNS system in the AOS product implements preemptive and persistent caching of DNS records for voice signaling protocols. The VNS system maintains a table of DNS records in a cache for voice signaling protocols like SIP and MGCP. For example, if a request is generated from a SIP client (such as a SIP trunk or SIP proxy), for which there is a configured SIP server entity (such as a proxy address or SIP server address), the request is always serviced from the local DNS cache (rather than from an external DNS server). This ensures that SIP access to DNS is always available immediately, even during transient DNS outages.

The VNS system in AOS can be configured manually by adding a host to the cache (using the command *voip name-service host on page 1984*) and by specifying the number of attempts used by VNS to verify the DNS cache changes (using the command *voip name-service verification attempts <number> interval <seconds> on page 1986*). You can view the VNS cache by using the commands *show voip name-service cache on page 1108* and *show voip name-service name-table on page 1109*.

Configuring an FQDN using the **voip name-service host** command forces the FQDN resolution (using DNS) to never timeout from the DNS name table. Each DNS record has a time to live (TTL) value that specifies the amount of time to cache the record. After this time, the DNS table (by default) removes the record from the cache. VNS issues DNS queries in an attempt to keep voice-related records cached in the DNS name table, but if the DNS name servers are not available, the records can expire from the DNS name table. The records associated with configured VNS host FQDNs are not flushed from the cache regardless of the TTL or age of the record, but rather are permanently cached dynamic resolutions.

Command History

Release A4.03	Command was introduced.
Release R11.5.0	Command was expanded to include the **tls** and **srv** configuration parameters.

Usage Examples

The following example adds the SIP host **example.user.net** to the VNS/DNS cache, using **TCP** requests:

(config)**#voip name-service host example.user.net sip tcp**

The following example configures TLS as the transport protocol for a statically added VNS host:(config)#voip name-service host example.user.net sip tls

voip name-service verification attempts <*number*> interval <*seconds*>

Use the **voip name-service verification attempts interval** command to configure the Voice over Internet Protocol (VoIP) name service (VNS) to verify any domain naming system (DNS) changes to the VNS table. Using the **no** form of this command disables verification.

Syntax Description

attempts <*number*>	Specifies the number of consecutive DNS answers that validate a change to the VNS table. Valid range is **1** to **10**.
interval <*seconds*>	Specifies the time interval (in seconds) to wait between verification attempts. Valid range is **1** to **600** seconds.

Default Values

By default, the VNS system does not verify DNS changes.

Functional Notes

Voice and media signaling protocols (such as SIP) often rely on DNS in order to ease configuration and administration of endpoints and also to implement redundancy mechanisms provided by DNS service records. Because voice and media signaling protocols are often directly coupled to a user experience, applications are often very sensitive to latency introduced by the DNS mechanism.

AOS voice products rely on the ability to resolve names to one or more service or address records quickly in order to place a call or register to an external voice server. The DNS server is often not local to the AOS unit, and it is not guaranteed to be accessible, even when other mechanisms necessary for successful call completion may be available. A DNS request for a particular host name results in local caching by the AOS unit, after which the DNS information is quickly available without requiring additional requests. The cache remains populated until the cached record expires.

The VNS system in the AOS product implements preemptive and persistent caching of DNS records for voice signaling protocols. The VNS system maintains a table of DNS records in a cache for voice signaling protocols like Session Initiation Protocol (SIP) and Media Gateway Control Protocol (MGCP). For example, if a request is generated from a SIP client (such as a SIP trunk or SIP proxy), for which there is a configured SIP server entity (such as a proxy address or SIP server address), the request is always serviced from the local DNS cache (rather than from an external DNS server). This ensures that SIP access to DNS is always available immediately, even during transient DNS outages.

The VNS system in AOS can be configured manually by adding a host to the cache (using the command *voip name-service host on page 1984*) and by specifying the number of attempts used by VNS to verify the DNS cache changes (using the command *voip name-service verification attempts <number> interval <seconds> on page 1986*). You can view the VNS cache by using the commands *show voip name-service cache on page 1108* and *show voip name-service name-table on page 1109*.

Command History

Release A4.03	Command was introduced.

Usage Examples

In the following example, the VNS system is configured to use **3** attempts to validate a DNS change, with **30** seconds between each attempt:

(config)**#voip name-service verification attempts 3 interval 30**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the **frame-relay 1.16** interface to the VRF instance named **RED**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#vrf forwarding RED**

vrf <*name*> route-distinguisher

Use the **vrf route-distinguisher** command to create a nondefault virtual routing and forwarding (VRF) instance and assign it a route distinguisher. Use the **no vrf** command to remove all VRF instances configured on the system. Use the **no vrf route-distinguisher** command to destroy the VRF instance and any commands configured on the VRF. Variations of this command include:

vrf <*name*> **route-distinguisher as-2byte** <*ASN:nn*>
vrf <*name*> **route-distinguisher as-4byte** <*ASN:nn*>
vrf <*name*> **route-distinguisher ip** <*ipv4 address:nn*>
vrf system-control route-distinguisher as-2byte 0:1
vrf system-management route-distinguisher as-2byte 0:2

Syntax Description

<*name*>	Specifies the name of the VRF instance. Valid range is up to **79** alphanumeric characters.
as-2byte <*ASN:nn*>	Specifies the autonomous system number (ASN)-relative route distinguisher as a 16-bit AS number *(ASN)* and a 32-bit arbitrary number (*nn*).
as-4byte <*ASN:nn*>	Specifies the ASN-relative route distinguisher as a 32-bit AS number (*ASN)* and a 16-bit arbitrary number (*nn*).
ip <*ipv4 address:nn*>	Specifies an IPv4 address-relative route distinguisher, which consists of an IPv4 address and a 16-bit arbitrary number (*nn*). IPv4 addresses should be expressed in decimal dotted notation (for example, **10.10.10.1**).
system-control	Specifies the system control VRF instance.
system-management	Specifies the system management VRF instance.

Default Values

No default values are necessary for this command.

Command History

Release 16.1	Command was introduced.
Release 18.3	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran internetworking products. In addition, the **as-2byte**, **as-4byte**, and **ip** <*ipv4 address:nn*> parameters were added.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for IPv6 support in Adtran voice products. In addition, the **as-2byte**, **as-4byte**, and **ip** <*ipv4 address:nn*> parameters were added.
Release R10.10.0	Command was expanded to include the **system-control** and **system-management** options.

Functional Notes

The route distinguisher **0:0** or **0.0.0.0:0** is reserved for the default (unnamed) VRF instance and cannot be reassigned. Additionally, the VRF names **system-control** and **system-management** use route distinguishers **0:1** and **0:2** respectively, and cannot be reassigned. The system control and system management VRF instances exist by default and cannot be removed. These VRFs exist for the system control Ethernet virtual connection (EVC) and the system management EVC. Refer to *System Control EVC Command Set on page 3745* and *System Management EVC Command Set on page 3843* for more information.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Once a nondefault VRF is created, it must be assigned to the appropriate interfaces. Use the *voip name-service host on page 1984* to assign interfaces to the VRF. By default, interfaces are assigned to the default unnamed VRF. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

Usage Examples

The following example creates the VRF **Red** and assigns the 2-byte route distinguisher **2:2**:

(config)**#vrf RED route-distinguisher as-2byte 2:2**

APPLICATION COMMAND SETS

This section includes the following command sets:

NETWORK SYNC APPLICATION COMMAND SET

Use the network synchronization (Network Sync) application command set to aid in troubleshooting Network Sync configuration on the AOS unit. Network Sync application commands do not affect the configuration of the AOS unit, and they do not persist between reboots. To access the Network Sync application command set, enter the **application** command from the Enable mode prompt, and then enter the appropriate Network Sync application command as follows (refer to the command *application on page 98*):

```
>enable
#application
(app)#
```

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

exit on page 83

Commands for this command set are described in this section in alphabetical order.

network-sync source-override on page 1993
network-sync transmit-ssm-override <input> on page 1994
network-sync wait-to-restore clear on page 1996

network-sync source-override

Use the **network-sync source-override** command to override the current clock source. When the clock source override is activated, there is a line displayed in the command **show network-sync** that indicates the override is active. Use the **no** form of this command to cancel the clock override. Variations of this command include:

network-sync source-override cancel
network-sync source-override internal
network-sync source-override primary
network-sync source-override primary force
network-sync source-override secondary
network-sync source-override secondary force

Syntax Description

cancel	Specifies that the source override is cancelled. This functions exactly the same as using the **no** command.
internal	Specifies that the internal oscillator is selected as the current clock source.
primary	Specifies that the primary clock source is overridden.
secondary	Specifies that the secondary clock source is overridden.
force	Optional. Specifies that the primary or secondary clock source should be selected as the current clock even if it is down.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example overrides the secondary clock source:

#application
(app)**#network-sync source-override secondary**

network-sync transmit-ssm-override <*input*>

Use the **network-sync transmit-ssm-override** command to create an unconditional override of the synchronization status message (SSM) configuration for the clock. This command is used primarily for testing purposes. Use the **no** form of this command to remove the override.

Syntax Description

<*input*>	Specifies the SSM quality level override option. Refer to the Functional Notes of this command for specifics.

Default Values

By default, SSM override options are those provided by Ethernet equipment clock (EEC) option 2.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

The various <*input*> parameters available for SSM override vary according to the EEC option selected in the Network Sync configuration (refer to *eec-option on page 4437*). If you have not specified an EEC option, option 2 is used by default. The following tables outline the <*input*> parameters for the **network-sync transmit-ssm-override** command.

Table 1. SSM Override Parameters for EEC Option 1

SSM Override Parameter	Description
q1-dnu	Do Not Use for Synchronization (0xF)
q1-eec1	Synchronous digital hierarchy (SDH) Equipment Clock (0xB)
q1-prc	Primary Reference Clock (0x2)
q1-ssu-a	Primary Level Synchronization Supply Unit (0x4)
q1-ssu-b	Second Level Synchronization Supply Unit (0x8)
<*input*>	Enter SSM as a decimal or hexadecimal value

Table 2. SSM Override Parameters for EEC Option 2

SSM Override Parameter	Description
q1-dus	Do Not Use for Synchronization (0xF)
q1-eec2	Stratum 3 Traceable (0xA)
q1-prov	Provisioned by Network Operator (0xE)

Table 2. SSM Override Parameters for EEC Option 2 (Continued)

SSM Override Parameter	Description
q1-prs	Stratum 1 Traceable (0x1)
q1-smc	SONET Minimum Clock Traceable (0xC)
q1-st2	Stratum 2 Traceable (0x7)
q1-st3e	Stratum 3E Traceable (0xD)
q1-stu	Synchronized Traceability Unknown (0x0)
q1-tnc	Transit Node Clock Traceable (0x4)
<input>	Enter SSM as a decimal or hexadecimal value

Usage Examples

The following example creates an unconditional SSM override:

#application
(app)**#network-sync transmit-ssm-override q1-dnu**

network-sync wait-to-restore clear

Use the **network-sync wait-to-restore clear** command to clear the wait-to-restore timers. Variations of this command include:

network-sync wait-to-restore clear primary
network-sync wait-to-restore clear secondary

Syntax Description

primary	Specifies the primary timers are cleared.
secondary	Specifies the secondary timers are cleared.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example clears the primary wait-to-restore timers:

#application
(app)**#network-sync wait-to-restore clear primary**

Y.1731 Application Command Set

Use the Y.1731 application command set to configure and verify specifics of Y.1731 configuration on the AOS unit. Y.1731 applications are used in one- and two-way frame delay performance monitoring sessions, as well as frame loss monitoring sessions. To access the Y.1731 application command set, enter the **application** command from the Enable mode prompt, and then enter the appropriate Y.1731 application command as follows (refer to the command *application on page 98*):

```
>enable
#application
(app)#ethernet y1731 meg char-string MEG 3 100
(app-y1731 MEG)#
```

In AOS Release 17.1, output modifiers were introduced for all **show** commands. These modifiers help specify the information displayed in the **show** command output. The modifiers are appended to the end of the **show** command, preceded by the pipe character (|), and followed by the <*text*> to **exclude**, **include**, or with which to **begin** the display. The following output modifiers are common for all **show** commands:

| begin <*text*>	Produces output that begins with lines, including the specified text and every line thereafter.
| exclude <*text*>	Produces output that excludes any lines containing the specified text.
| include <*text*>	Produces output that only displays lines with the specified text.

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

exit on page 83

All other commands for this command set are described in this section in alphabetical order:

frame-delay one-way on page 1998
frame-delay two-way on page 2000
frame-loss single-ended on page 2002
frame-loss synthetic single-ended on page 2004
linktrace <mep id | target mac address> on page 2007
loopback on page 2008
show frame-delay one-way on page 2010
show frame-delay two-way on page 2012
show frame-loss single-ended on page 2014
show frame-loss synthetic single-ended on page 2016
show loopback multicast on page 2018

frame-delay one-way

Use the **frame-delay one-way** command to configure a Y.1731 one-way frame delay performance monitoring session between maintenance entity group (MEG) endpoints (MEPs). Use the **no** form of this command to disable the frame delay monitoring session. Variations of this command include:

frame-delay one-way <*mep id* | *target mac address* | **multicast**>
frame-delay one-way <*mep id* | *target mac address* | **multicast**> **priority** <*value*>
frame-delay one-way <*mep id* | *target mac address* | **multicast**> **priority** <*value*> **count** <*value*>
frame-delay one-way <*mep id* | *target mac address* | **multicast**> **priority** <*value*> **count** <*value*> **interval** <*interval*>
frame-delay one-way <*mep id* | *target mac address* | **multicast**> **priority** <*value*> **count** <*value*> **interval** <*interval*> **size** <*bytes*>
frame-delay one-way <*mep id* | *target mac address* | **multicast**> **priority** <*value*> **count** <*value*> **interval** <*interval*> **size** <*bytes*> **data** <*data*>
frame-delay one-way <*mep id* | *target mac address* | **multicast**> **priority** <*value*> **count** <*value*> **interval** <*interval*> **size** <*bytes*> **data** <*data*> **verbose**

Syntax Description

<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191.**
<*target mac address*>	Specifies the medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
priority <*value*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.
count <*value*>	Optional. Specifies the number of one-way delay measurement message frames (1DM) sent to the target MEP. Valid range is **2** to **1024**.
interval <*interval*>	Optional. Specifies the time (in milliseconds) between 1DM transmissions. Valid range is **100** to **900000** ms.
size <*bytes*>	Optional. Specifies the size of the 1DM frame in bytes. If no size is specified, 1DM fames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the 1DM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.
data <*data*>	Optional. Specifies a hex pattern used to fill the data TLV. Valid range is **0x0000** to **0xFFFF**.
verbose	Optional. Specifies details are given in the monitoring session.

Default Values

By default, no one-way frame delay monitoring sessions are configured. If a session is configured, it has an interval of **1000** ms, a size of **0** bytes, and a data pattern of **0x0000** by default.

Command History

Release R10.10.0	Command was introduced.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a one-way frame delay monitoring session for MEP **100** with a priority of **3**, a count of **100**, and the default interval, size, and data values:

#application
(app)**#ethernet y1731 meg char-string MEG 3 100**
(app-y1731 MEG)#f**rame-delay one-way 100 priority 3 count 100**

frame-delay two-way

Use the **frame-delay two-way** command to configure a Y.1731 two-way frame delay performance monitoring session between maintenance entity group (MEG) endpoints (MEPs). Use the **no** form of this command to disable the frame delay monitoring session. Variations of this command include:

frame-delay two-way <*mep id* | *target mac address* | **multicast**>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **count** <*count*>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **data** <*data*>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **interval** <*interval*>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **measurement-interval** <*measurement interval*>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **priority** <*priority*>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **repetition-time** <*repetition time*>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **size** <*size*>
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **start-time [**<*start time*> **| immediate]**
frame-delay two-way <*mep id* | *target mac address* | **multicast**> **stop-time** <*stop time*>

NOTE *After specifying the MEP ID, MAC, or multicast address of the target MEP(s), the other parameters can be entered in any order.*

Syntax Description

<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191**.
<*target mac address*>	Specifies the medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
count <*count*>	Optional. Specifies the number of delay measurement messages (DMMs) sent to the target MEP. Cannot be used in conjunction with the **stop-time** parameter. Must be greater than or equal to the **measurement interval** divided by the **interval**. Valid range is **2** to **1024**.
data <*data*>	Optional. Specifies a hex pattern used to fill the data TLV. Valid range is **0x0000** to **0xFFFF**.
interval <*interval*>	Optional. Specifies the number of milliseconds between DMM transmissions. Valid range is **100** to **900000** ms.
measurement-interval <*measurement interval*>	Optional. Specifies the number of seconds over which frame delay statistics are generated. If used with the **repetition-time** parameter, must be in minute intervals (multiples of 60) and less than the repetition time. Valid range is **60** to **86400** seconds.
priority <*priority*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.

repetition-time <*repetition time*>	Optional. Specifies the number of seconds between the start time of measurement intervals. The repetition time must be at least as long as the measurement interval and must be in minute intervals (multiples of 60). Valid range is **60** to **86400** seconds.
size <*size*>	Optional. Specifies the size in bytes of the DMM frame. If no size is specified, DMM fames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the DMM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.
start-time	Optional. Specifies the start time of the monitoring session.
<*start time*>	Specifies the absolute time of day after the initiation of the session that the measurement interval will begin. Specified in the format **HH:MM:SS**. For example, midnight is **00:00:00**.
immediate	Specifies that the session will start immediately.
stop-time <*stop-time*>	Optional. Specifies the duration in seconds of the frame delay monitoring session. Cannot be used in conjunction with the **count** parameter. Must be greater than or equal to the interval and must be large enough for one packet to be transmitted. If **stop-time** is not defined, then **count** will be used. Valid range is **0** to **15552000** seconds.

Default Values

By default, no two-way frame delay monitoring sessions are configured. If a session is configured, it has a count of **60**, an interval of **1000** ms, a measurement interval of **60** seconds, a size of **0** bytes, and a data pattern of **0x0000** by default.

Command History

Release R10.10.0	Command was introduced.
Release R11.6.0	Command was expanded to include the **repetition-time**, **start-time** and **stop-time** parameters.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a two-way frame delay monitoring session for MEP **100** with a priority of **3**, a start time of **02:00:00** (2:00 A.M.), a stop time of **3600** seconds (one hour), and the default interval, measurement interval, repetition time, size, and data values:

#application
(app)**#ethernet y1731 meg char-string MEG 3 100**
(app-y1731 MEG)**#frame-delay two-way 100 priority 3 start-time 02:00:00 stop-time 3600**

frame-loss single-ended

Use the **frame-loss single-ended** command to monitor single-ended frame loss across maintenance entity group (MEG) endpoints (MEPs). This commands uses actual data traffic to measure frame loss. To measure frame loss using synthetic frames, use the *frame-loss synthetic single-ended on page 2004*. Use the **no** form of this command to disable the monitoring feature. Variations of this command include:

frame-loss single-ended <*mep id* | *target mac address* | **multicast**>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **count** <*count*>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **data** <*data*>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **interval** <*interval*>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **measurement-interval** <*measurement interval*>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **priority** <*priority*>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **repetition-time** <*repetition time*>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **size** <*size*>
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **start-time [**<*start time*> **| immediate]**
frame-loss single-ended <*mep id* | *target mac address* | **multicast**> **stop-time** <*stop time*>

After specifying the MEP ID, MAC, or multicast address of the target MEP(s), the other parameters can be entered in any order.

Syntax Description

<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191**.
<*target mac address*>	Specifies medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
count <*count*>	Optional. Specifies the number of loss measurement messages (LMMs) sent to the target MEP. Cannot be used in conjunction with the **stop-time** parameter. Must be greater than or equal to the **measurement interval** divided by the **interval**. Valid range is **2** to **1024**.
data <*data*>	Optional. Specifies a hex pattern used to fill the data TLV. Valid range is **0x0000** to **0xFFFF**.
interval <*interval*>	Optional. Specifies the number of milliseconds between DMM transmissions. Valid range is **100** to **900000** ms.
measurement-interval <*measurement interval*>	Optional. Specifies the number of seconds over which frame loss statistics are generated. If used with the **repetition-time** parameter, must be in minute intervals (multiples of 60) and less than the repetition time. Valid range is **60** to **86400** seconds.

priority <*priority*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.
repetition-time <*repetition time*>	Optional. Specifies the number of seconds between the start time of measurement intervals. The repetition time must be at least as long as the measurement interval and must be in minute intervals (multiples of 60). Valid range is **60** to **86400** seconds.
size <*size*>	Optional. Specifies the size in bytes of the DMM frame. If no size is specified, DMM fames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the DMM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.
start-time	Optional. Specifies the start time of the monitoring session.
<*start time*>	Specifies the absolute time of day after the initiation of the session that the measurement interval will begin. Specified in the format **HH:MM:SS**. For example, midnight is **00:00:00**.
immediate	Specifies that the session will start immediately.
stop-time <*stop-time*>	Optional. Specifies the duration in seconds of the frame delay monitoring session. Cannot be used in conjunction with the **count** parameter. Must be greater than or equal to the interval and must be large enough for one packet to be transmitted. If **stop-time** is not defined, then **count** will be used. Valid range is **0** to **15552000** seconds.

Default Values

By default, no two-way frame delay monitoring sessions are configured. If a session is configured, it has a count of **60**, an interval of **1000** ms, a measurement interval of **60** seconds, a size of **0** bytes, and a data pattern of **0x0000** by default.

Command History

Release R10.10.0	Command was introduced.
Release R11.6.0	Command was expanded to include the **repetition-time**, **start-time** and **stop-time** parameters.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a frame-loss monitoring session for MEP **100** with a priority of **3**, a start time of **02:00:00** (2:00 A.M.), a stop time of **3600** seconds (one hour), and the default interval, measurement interval, repetition time, size, and data values:

#application
(app)**#ethernet y1731 meg char-string MEG 3 100**
(app-y1731 MEG)**#frame-loss single-ended 100 priority 3 start-time 02:00:00 stop-time 3600**

frame-loss synthetic single-ended

Use the **frame-loss synthetic single-ended** command to monitor frame loss across maintenance entity group (MEG) endpoints (MEPs). This commands uses synthetic frames to measure frame loss. To measure frame loss using actual data fames, use the *frame-loss single-ended on page 2002*.Use the **no** form of this command to disable the monitoring feature. Variations of this command include:

frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **count** <*count*>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **data** <*data*>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **interval** <*interval*>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **measurement-interval** <*measurement interval*>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **priority** <*priority*>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **repetition-time** <*repetition time*>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **size** <*size*>
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **start-time [**<*start time*> **| immediate]**
frame-loss synthetic single-ended <*mep id* | *target mac address* | **multicast**> **stop-time** <*stop time*>

After specifying the MEP ID, MAC, or multicast address of the target MEP(s), the other parameters can be entered in any order.

Syntax Description

<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191**.
<*target mac address*>	Specifies the medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
count <*count*>	Optional. Specifies the number of synthetic loss messages (SLMs) sent to the target MEP. Cannot be used in conjunction with the **stop-time** parameter. Must be greater than or equal to the **measurement interval** divided by the **interval**. Valid range is **2** to **1024**.
data <*data*>	Optional. Specifies a hex pattern used to fill the data TLV. Valid range is **0x0000** to **0xFFFF**.
interval <*interval*>	Optional. Specifies the number of milliseconds between DMM transmissions. Valid range is **100** to **900000** ms.
measurement-interval <*measurement interval*>	Optional. Specifies the number of seconds over which frame loss statistics are generated. If used with the **repetition-time** parameter, must be in minute intervals (multiples of 60) and less than the repetition time. Valid range is **60** to **86400** seconds.

priority <*priority*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.
repetition-time <*repetition time*>	Optional. Specifies the number of seconds between the start time of measurement intervals. The repetition time must be at least as long as the measurement interval and must be in minute intervals (multiples of 60). Valid range is **60** to **86400** seconds.
size <*size*>	Optional. Specifies the size in bytes of the DMM frame. If no size is specified, DMM fames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the DMM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.
start-time	Optional. Specifies the start time of the monitoring session.
<*start time*>	Specifies the absolute time of day after the initiation of the session that the measurement interval will begin. Specified in the format **HH:MM:SS**. For example, midnight is **00:00:00**.
immediate	Specifies that the session will start immediately.
stop-time <*stop-time*>	Optional. Specifies the duration in seconds of the frame delay monitoring session. Cannot be used in conjunction with the **count** parameter. Must be greater than or equal to the interval and must be large enough for one packet to be transmitted. If **stop-time** is not defined, then **count** will be used. Valid range is **0** to **15552000** seconds.

Default Values

By default, no two-way frame delay monitoring sessions are configured. If a session is configured, it has a count of **60**, an interval of **1000** ms, a measurement interval of **60** seconds, a size of **0** bytes, and a data pattern of **0x0000** by default.

Command History

Release R10.10.0	Command was introduced.
Release R11.6.0	Command was expanded to include the **repetition-time**, **start-time** and **stop-time** parameters.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a synthetic frame-loss monitoring session for MEP **100** with a priority of **3**, a start time of **02:00:00** (2:00 A.M.), a stop time of **3600** seconds (one hour), and the default interval, measurement interval, repetition time, size, and data values:

#application
(app)**#ethernet y1731 meg char-string MEG 3 100**
(app-y1731 MEG)**#frame-loss synthetic single-ended 100 priority 3 start-time 02:00:00 stop-time 3600**

linktrace *<mep id | target mac address>*

Use the **linktrace** command to trace the link between Y.1731 maintenance entity group (MEG) endpoints (MEPs). Use the **no** form of this command to disable the trace feature. Variations of this command include:

linktrace *<mep id | target mac address>*
linktrace *<mep id | target mac address>* **sorted**
linktrace *<mep id | target mac address>* **ttl** *<value>*
linktrace *<mep id | target mac address>* **ttl** *<value>* **mac-fdb-only**
linktrace *<mep id | target mac address>* **ttl** *<value>* **mac-fdb-only sorted**
linktrace *<mep id | target mac address>* **ttl** *<value>* **verbose**

Syntax Description

<mep id | target mac address>	Specifies the MEP ID or medium access control (MAC) address of the target MEP. Valid MEP ID range is **1** to **8191**. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
sorted	Optional. Sorts the results of the trace by MEP ID or MAC address.
ttl *<value>*	Optional. Specifies the number of mapped IP (MIP) address hops. Valid range is **1** to **255**.
mac-fdb-only	Optional. Specifies that only MAC addresses in the forwarding database (FDB) are traced.
verbose	Optional. Specifies that trace results are shown in detail.

Default Values

By default, link trace tests are not performed.

Command History

Release R10.10.0	Command was introduced.

Usage Example

The following example executes a trace of the link between MEP **100** and MEP **500**:

#application
(app)**#ethernet y1731 meg char-string MEG 3 100**
(app-y1731 MEG)**#linktrace 500**

loopback

Use the **loopback c**ommand to send loopback messages (LBMs) between Y.1731 maintenance entity group (MEG) endpoints (MEPs). The LBMs are used to verify bidirectional connectivity. Use the **no** form of this command to disable this feature. Variations of this command include:

loopback multicast
loopback multicast priority <*value*>
loopback multicast priority <*value*> **count** <*value*>
loopback multicast priority <*value*> **count** <*value*> **interval** <*interval*>
loopback multicast priority <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*>
loopback multicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*>
loopback multicast priority <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random]**
loopback multicast priority <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random] validate**
loopback multicast priority <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random] validate verbose**
loopback multicast priority <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random] verbose**

loopback unicast <*mep id* | *target mac address*>
loopback unicast <*mep id* | *target mac address*> **priority** <*value*>
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*>
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*>
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*>
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*>
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random]**
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random] validate**
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random] validate verbose**
loopback unicast <*mep id* | *target mac address*> **priority** <*value*> **count** <*value*> **interval** <*interval*> **timeout** <*value*> **size** <*value*> **data [hex:4 | random] verbose**

Syntax Description

multicast	Specifies the session is configured for multicast.
unicast <*mep id* | *target mac address*>	Specifies the unicast MEP ID or medium access control (MAC) address of the target MEP. Valid MEP ID range is **1** to **8191**. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.

priority *<value>*	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.
count *<value>*	Optional. Specifies the number of LBMs sent to the target MEP. Valid range is **2** to **1024**.
interval *<interval>*	Optional. Specifies the time (in milliseconds) between LBM transmissions. Valid range is **100** to **10000** ms.
timeout *<value>*	Optional. Specifies the interval at which the loopback feature times out if there is no response to an LBM. Valid range is **100** to **5000** milliseconds.
size *<bytes>*	Optional. Specifies the size of the LBM frame in bytes. If no size is specified, LBM fames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the LBM frame is the correct length. Valid range is **64** to **9242** bytes.
data	Optional. Specifies a pattern used to fill the data TLV.
hex:4	Specifies any sequence of 4 hexadecimal digits.
random	Specifies a pseudo randomly generated number pattern
validate	Optional. Validates the connection between the MEPs.
verbose	Optional. Specifies that details are included in loopback test results.

Default Values

By default, no loopback tests are configured. If a test is configured, it has an interval of **1000** ms, a timeout of **100** seconds, a size of **0** bytes, and a data pattern of **0x0000** by default.

Command History

Release R10.10.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **random** parameter.
Release R11.7.0	The valid range of the **size** parameter was changed from **64** to **2000** bytes to **64** to **9242** bytes.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Functional Notes

When using the multicast loopback option, LBMs are sent a multicast MAC address. Up to 8 responding (LBR) MEPs/MAC addresses are recorded and displayed in the output of the command *show loopback multicast on page 2018*. The maximum count of LBMs supported for **multicast** is **60**, and the maximum for unicast is **1024**.

Usage Examples

The following example creates a loopback test between MEP **100** and MEP **500**:

#application
(app)**#ethernet y1731 meg char-string MEG 3 100**
(app-y1731 MEG)**#loopback unicast 500**

show frame-delay one-way

Use the **show frame-delay one-way** command to display statistics and configuration of one-way frame delay performance monitoring sessions. Variations of this command include:

show frame-delay one-way
show frame-delay one-way <*session id*>
show frame-delay one-way <*session id*> **realtime**

*The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*

For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.

Syntax Description

<*session id*>	Optional. Specifies that results for a specific frame delay monitoring session are displayed. Valid range is **1** to **n**.
realtime	Optional. Displays full-screen output in realtime. Information is continuously updated on the console.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example displays the configuration of all one-way frame delay monitoring sessions:

```
#application
(app)#ethernet y1731 meg char-string MEG 3 100
(app-y1731 MEG)#show frame-delay one-way
Session 1 is Active
Source MAC                  : 00:a0:c8:00:00:01
VLAN Priority               : 7
Receive Interval            ms: 1000.12
Measurement Interval
Receive Count               Previous        Current
                            : 60            55
```


Delay		
Mean	ms: 0.08	0.09
Maximum	ms: 0.10	0.21
Minimum	ms: 0.07	0.07
Delay Variation Maximum		
Inter-packet	ms: 0.03	0.13
Reference-packet	ms:0.03	0.14

show frame-delay two-way

Use the **show frame-delay two-way** command to display statistics and configuration of two-way frame delay performance monitoring sessions. Variations of this command include:

show frame-delay two-way
show frame-delay two-way *<session id>*
show frame-delay two-way *<session id>* **realtime**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

<session id>	Optional. Specifies that results for a specific frame delay monitoring session are displayed. Valid range is **1** to **n**.
realtime	Optional. Displays full-screen output in realtime. Information is continuously updated on the console.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.
Release R11.6.0	Command output was expanded to include the **Start-Time**, **Stop-Time**, **Repetition-Time**, and **Suspect Flag** fields.

Usage Examples

The following example displays the configuration of all two-way frame delay monitoring sessions:

#application
(app)**#ethernet y1731 meg char-string MEG 3 100**
(app-y1731 MEG)**#show frame-delay two-way**
MEP 100 Two-way Delay Session Results
Session 1 is Active

Session Type	: Proactive
Target MAC	: 00:a0:c8:01:00:00
VLAN Priority	: 3
Start Time	: 12:01:10 UTC Thu Jan 01 197
Stop Time	: Forever
DMM Transmit Interval	: 1000

DMM Measurement Interval	: 60	
Repetition Time	: 60	
DMM Size	: 0	
DMM Payload Data	: 0000	
Measurement Interval	Previous	Current
DMMs Transmitted	: 60	28
DMRs Received	: 0	0
Valid DMRs Received	: 0	0
Invalid DMRs Received	: 0	0
Out-of-order DMRs Received	: 0	0
Suspect Flag	: No	No
Round-trip Delay		
Mean	ms: 0.00	0.00
Maximum	ms: 0.00	0.00
Minimum	ms: 0.00	0.00
Round-trip Delay Variation Mean		
Inter-packet	ms: 0.00	0.00
Round-trip Delay Variation Maximum		
Inter-packet	ms: 0.00	0.00
Reference-packet	ms: 0.00	0.00
Round-trip Delay Variation Minimum		
Inter-packet	ms: 0.00	0.00
Forward One-Way Delay		
Mean	ms: 0.00	0.00
Maximum	ms: 0.00	0.00
Minimum	ms: 0.00	0.00
Forward One-Way Delay Variation Mean		
Inter-packet	ms: 0.00	0.00
Forward One-Way Delay Variation Maximum		
Inter-packet	ms: 0.00	0.00
Forward One-Way Delay Variation Minimum		
Inter-packet	ms: 0.00	0.00
Backward One-Way Delay		
Mean	ms: 0.00	0.00
Maximum	ms: 0.00	0.00
Minimum	ms: 0.00	0.00
Backward One-Way Delay Variation Mean		
Inter-packet	ms: 0.00	0.00
Backward One-Way Delay Variation Maximum		
Inter-packet	ms: 0.00	0.00
Backward One-Way Delay Variation Minimum		
Inter-packet	ms: 0.00	0.00

show frame-loss single-ended

Use the **show frame-loss single-ended** command to display statistics of single-ended frame loss monitoring sessions. Variations of this command include:

show frame-loss single-ended
show frame-loss single-ended <*session id*>
show frame-loss single-ended <*session id*> **realtime**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

> *Using the **realtime** argument for this command can adversely affect the performance or your unit.*

Syntax Description

<*session id*>	Optional. Specifies that results for a specific frame delay monitoring session are displayed. Valid range is **1** to **n**.
realtime	Optional. Displays full-screen output in real time. Information is updated on the console.

Default Values

No default values are necessary for this command.

Command History

Release R11.6.0	Command was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <number> on page 1133*).

Usage Examples

The following example displays the statistics of frame loss monitoring for session **1**:

#application
(app)**#ethernet y1731 meg char-string MEG 3 1111**
(app-y1731 MEG)**#show frame-loss single-ended 1**
MEP 1111 Single-Ended Frame Loss Results

Session 1 is Active

Session Type	: Proactive	
Target MAC	: 00:a0:c8:01:00:00	
VLAN Priority	: 4	
Start Time	: 12:06:46 UTC Thu Jan 01 1970	
Stop Time	: Forever	
LMM Transmit Interval	: 1000	
LMM Measurement Interval	: 60	
Repetition Time	: 60	
LMM Size	: 0	
LMM Payload Data	: 0000	
Measurement Interval	Previous	Current
LMMs Transmitted	: 60	56
LMRs Received	: 60	56
Valid LMRs Received	: 60	56
Invalid LMRs Received	: 0	0
Out-of-order LMRs Received	: 0	0
Suspect Flag	: No	No
Frame Loss Near End	: 0	0
Frame Loss Far End	: 0	0
Frame Loss Ratio Near End	: 0.0000	0.0000
Frame Loss Ratio Far End	: 0.0000	0.0000
Min Frame Loss Ratio Near End	: 0.0000	0.0000
Min Frame Loss Ratio Far End	: 0.0000	0.0000
Max Frame Loss Ratio Near End	: 0.0000	0.0000
Max Frame Loss Ratio Far End	: 0.0000	0.0000
Max Consecutive Frame Loss	: 0	0

show frame-loss synthetic single-ended

Use the **show frame-loss synthetic single-ended** command to display statistics of synthetic single-ended frame loss monitoring sessions. Variations of this command include:

show frame-loss synthetic single-ended
show frame-loss synthetic single-ended <*session id*>
show frame-loss synthetic single-ended <*session id*> **realtime**

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

> *Using the **realtime** argument for this command can adversely affect the performance or your unit.*

Syntax Description

<*session id*>	Optional. Specifies that results for a specific frame delay monitoring session are displayed. Valid range is **1** to **n**.
realtime	Optional. Displays full-screen output in realtime. Information is continuously updated on the console.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.
Release R11.6.0	Command output was expanded to include the **Start-Time**, **Stop-Time**, **Repetition-Time**, and **Suspect Flag** fields.

Usage Examples

The following example displays the statistics of synthetic frame loss monitoring for session **1**:

#application
(app)**#ethernet y1731 meg char-string MEG 3 1111**
(app-y1731 MEG)**#show frame-loss synthetic single-ended 1**
MEP 1111 Synthetic Single-Ended Frame Loss Results

Session 1 is Active

Session Type	: Proactive	
Target MAC	: 00:a0:c8:01:00:00	
VLAN Priority	: 4	
Start Time	: 12:06:46 UTC Thu Jan 01 1970	
Stop Time	: Forever	
SLM Transmit Interval	: 1000	
SLM Measurement Interval	: 60	
Repetition Time	: 60	
SLM Size	: 0	
SLM Payload Data	: 0000	
Measurement Interval	Previous	Current
SLMs Transmitted	: 60	56
SLRs Received	: 60	56
Valid SLRs Received	: 60	56
Invalid SLRs Received	: 0	0
Out-of-order SLRs Received	: 0	0
Suspect Flag	: No	No
Frame Loss Near End	: 0	0
Frame Loss Far End	: 0	0
Frame Loss Ratio Near End	: 0.0000	0.0000
Frame Loss Ratio Far End	: 0.0000	0.0000
Min Frame Loss Ratio Near End	: 0.0000	0.0000
Min Frame Loss Ratio Far End	: 0.0000	0.0000
Max Frame Loss Ratio Near End	: 0.0000	0.0000
Max Frame Loss Ratio Far End	: 0.0000	0.0000
Max Consecutive Frame Loss	: 0	0

show loopback multicast

Use the **show loopback multicast** command to display a detailed report of all remote Y.1731 maintenance entity group (MEG) endpoints (MEPs) that responded to the last issuance of the **loopback multicast** command (refer to *loopback on page 2008*).

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The output of this command is reset with every new issuance of the **loopback multicast** command (refer to *loopback on page 2008*). Only eight responding remote devices are displayed in the output of the **show loopback multicast** command, regardless of how many remote devices are configured or have learned medium access control (MAC) addresses.

Usage Examples

The following example displays output from the **show loopback multicast** command:

```
#application
(app)#ethernet y1731 meg char-string MEG 3 100
(app-y1731 MEG)#show loopback multicast
```

MacAddress	RMEP ID	Success	Out Of Order	Data Mismatch	Out	Timed Incomplete
00:00:12:AB:12:12	416	60	0	0	0	0
00:A0:C8:01:ED:A5	3416	60	0	0	0	0

INTERFACE COMMAND SETS

The interface command sets are divided into the following sections:

LINE INTERFACE COMMAND SETS

This section includes the following command sets:

LINE (CONSOLE) INTERFACE COMMAND SET

To activate the Line (Console) Interface Configuration mode, enter the **line console 0** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#line console 0
(config-con 0)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

access-attempts on page 2022
accounting commands begin on page 2023
authorization commands begin on page 2026
databits <value> on page 2028
flowcontrol on page 2029
line-timeout <value> on page 2030
login on page 2031
login authentication <listname> on page 2032
login local-userlist on page 2033
parity on page 2034
password <password> on page 2035
speed <rate> on page 2036
stopbits <value> on page 2037

access-attempts

Use the **access-attempts** command to specify the number of failed access attempts allowed on the line console before the session is locked. Use the **no** form of this command to disable this feature. Variations of this command include:

access-attempts <*number*>
access-attempts <*number*> **lock-period** <*number*>

Syntax Description

<*number*>	Specifies the number of failed access attempts allowed before the session is locked. The session remains locked for the lock period. Valid range is **1** to **10** attempts; a value of **0** disables the feature.
lock-period <*number*>	Optional. Specifies the lock period. Valid range is **1** to **30** seconds, with a default value of **3** seconds.

Default Values

By default, this feature is disabled and multiple access attempts are allowed. When enabled, the default lock period is **3** seconds.

Command History

Release R11.10.2	Command was introduced.

Usage Examples

The following example specifies that **5** failed login attempts are allowed before the session is locked, and that the session remains locked for **10** seconds:

(config)**#line console 0**
(config-con 0)**#access-attempts 5 lock-period 10**

accounting commands <*level*> <*listname*>

Use the **accounting commands** command to assign authentication, authorization, and accounting (AAA) command accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA command accounting method list from the interface. Variations of this command include:

accounting commands <*level*> **default**
accounting commands <*level*> <*listname*>

Syntax Description

<*level*>	Specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
default	Applies the default AAA command accounting method list to the interface.
<*listname*>	Applies the specified AAA command accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA command accounting method lists are used to specify the types of information recorded when users access specified command levels. For more information about configuring command accounting lists, refer to the command *aaa accounting connection on page 1157*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA command accounting list **Accounting1** is applied to all Level **15** commands on all console lines:

(config)**#line console 0**
(config-con 0)**#accounting commands 15 Accounting1**

accounting connection <*listname*>

Use the **accounting connection** command to assign authentication, authorization, and accounting (AAA) connection accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA connection accounting method list from the interface. Variations of this command include:

accounting connection default
accounting connection <*listname*>

Syntax Description

default	Applies the default AAA connection accounting method list to the interface.
<*listname*>	Applies the specified AAA connection accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA connection accounting method lists are used to specify the types of information recorded about outbound connections made from the AOS unit. For more information about configuring connection accounting lists, refer to the command *aaa accounting connection on page 1157*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA connection accounting list **AcctConn1** is applied to all console lines:

(config)**#line console 0**
(config-con 0)**#accounting connection AcctConn1**

accounting exec <*listname*>

Use the **accounting exec** command to assign authentication, authorization, and accounting (AAA) executive accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA executive accounting method list from the interface. Variations of this command include:

accounting exec default
accounting exec <*listname*>

Syntax Description

default	Applies the default AAA connection accounting method list to the interface.
<*listname*>	Applies the specified AAA connection accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA executive accounting method lists are used to specify the types of information recorded about inbound connections made by connecting to the line interfaces and creating a terminal session. For more information about configuring executive accounting lists, refer to the command *aaa accounting exec on page 1160*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA executive accounting list **Inboundacct1** is applied to the console line:

(config)**#line console 0**
(config-con 0)**#accounting exec Inboundacct1**

authorization commands *<level> <listname>*

Use the **authorization commands** command to assign authentication, authorization, and accounting (AAA) command authorization method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA command authorization method list from the interface. Variations of this command include:

authorization commands *<level>* **default**
authorization commands *<level> <listname>*

Syntax Description

<level>	Specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
default	Applies the default AAA command authorization method list to the interface.
<listname>	Applies the specified AAA command authorization method list to the interface.

Default Values

By default, no AAA command authorization method list is applied to the line interface.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA command authorization method lists are used to allow or restrict the use of certain commands on a per-user basis. For more information about configuring command authorization lists, refer to the command *aaa authorization commands <level> on page 1176*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA command authorization list **Authorization1** is applied to the Level **15** commands on all console line:

(config)**#line console 0**
(config-con 0)**#authorization commands 15 Authorization1**

authorization exec <*listname*>

Use the **authorization exec** command to assign authentication, authorization, and accounting (AAA) Enable mode authorization method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA Enable mode authorization method list from the interface. Variations of this command include:

authorization exec default
authorization exec <*listname*>

Syntax Description

default	Applies the default AAA Enable mode authorization method list to the interface.
<*listname*>	Applies the specified AAA Enable mode authorization method list to the interface.

Default Values

By default, no AAA Enable mode authorization method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA Enable mode authorization method lists are used to allow or restrict user access to the privileged command line interface (CLI) mode (Enable mode). For more information about configuring Enable mode authorization lists, refer to the command *aaa authorization exec on page 1181*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA Enable mode authorization list **ExecList1** is applied to the console line:

(config)**#line console 0**
(config-con 0)**#authorization exec ExecList1**

databits *<value>*

Use the **databits** command to set the number of databits per character for a terminal session. This value must match the configuration of your VT100 terminal or terminal emulator software. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the data bits per character. Select from **7** or **8** databits per character.

Default Values

By default, the databits are set to **8**.

Command History

Release 1.1	Command was introduced.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

This command is not available for vAOS instances.

Usage Examples

The following example configures **7** databits per character for the console terminal session:

(config)**#line console 0**
(config-con 0)**#databits 7**

flowcontrol

Use the **flowcontrol** command to set flow control for the line console. Use the **no** form of this command to return to the default setting. Variations of this command include:

flowcontrol none
flowcontrol software in

Syntax Description

none	Specifies no flow control.
software in	Configures AOS to derive flow control from the attached device.

Default Values

By default, flow control is set to **none**.

Command History

Release 3.1	Command was introduced.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

This command is not available for vAOS instances.

Usage Examples

The following example configures no flow control for the line console:

(config)**#line console 0**
(config-con 0)**#flowcontrol none**

line-timeout <*value*>

Use the **line-timeout** command to specify the number of minutes a line session may remain inactive before AOS terminates the session. Use the **no** form of this command to return to the default value. Variations of this command include:

line-timeout <*value*>
line-timeout <*value*> **any-activity**

Syntax Description

<*value*>	Specifies the number of minutes a line session may remain inactive before AOS terminates the session. Valid range: **0** to **35791**. Entering a **line-timeout** value of 0 disables the feature.
any-activity	Optional. Specifies that the SSH session does not time out until the specified value when the client is receiving or sending information with the AOS device.

Default Values

By default, the **line-timeout** is set to **15** minutes.

Command History

Release 11.1	Command was introduced.
Release R11.10.2	Command was expanded to include the **any-activity** parameter.

Functional Notes

The session timer is typically reset if data is sent from the client to the AOS device, but not if data is sent from the AOS device to the client. The optional **any-activity** parameter of this command prevents the session from timing out when the client is in a passive mode (only receiving data from the AOS device).

Usage Examples

The following example specifies a timeout of **2** minutes for all console sessions:

(config)**#line console 0**
(config-con 0)**#line-timeout 2**

login

Use the **login** command to enable security login on the line session. Additionally, it is necessary to configure the password using the command *password <password> on page 2035*. Use the **no** form of this command to disable the login feature.

Syntax Description

No subcommands.

Default Values

By default, secure login is disabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password (**mypassword**) on the available console session:

(config)**#line console 0**
(config-console 0)**#login**
(config-con 0)**#password mypassword**

login authentication <*listname*>

Use the **login authentication** command to apply the named authentication, authorization, and accounting (AAA) login method list to the line interface for authenticating users connecting to the interface. Use the **no** form of this command to remove the authentication method list from the interface.

Syntax Description

<*listname*>	Specifies the AAA login authentication method list to use for authentication.

Default Values

By default, no AAA login authentication method list is specified. If AAA is enabled (using the command *aaa on on page 1187*), but no login authentication method list is specified, the **default** login authentication method list is used. If the default list is used, but the default list has not been configured, console interfaces will automatically grant access (to prevent a lockout situation).

Command History

Release 5.1	Command was introduced.

Functional Notes

AAA login authentication method lists are used to verify user logins on the line interface. For more information about configuring login authentication method lists, refer to the command *aaa authentication login on page 1169*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the AAA login authentication method list **AuthList1** is applied to the console line:

```
(config)#line console 0
(config-con 0)#login authentication AuthList1
```


login local-userlist

Use the **login local-userlist** command to enable security login for the terminal session. It is required to configure user names and passwords using the **username/password** command from the Global Configuration mode (refer to *username <username> password <password> on page 1887*). Use the **no** form of this command to disable the login local-userlist feature.

*All user properties assigned using the **username/password** command are valid when using the **login local-userlist** command.*

Syntax Description

No subcommands.

Default Values

By default, there is no login password set to access the unit.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example displays creating a local userlist and enabling the security login feature on the **CONSOLE** port:

(config)**#username my_user password my_password**
(config)**#line console 0**
(config-con 0)**#login local-userlist**

When connecting to the unit, the following prompts are displayed:

User Access Login
Username: **Adtran**
Password:
Router#

parity

Use the **parity** command to specify the type of parity used as error correction. This value must match the configuration of your VT100 terminal or terminal emulator software. Use the **no** form of this command to return to the default value. Variations of this command include:

parity even
parity mark
parity none
parity odd
parity space

Syntax Description

even	Sets the parity bit to 0 if the number of 1 bits in the data sequence is odd, or set to 1 if the number of 1 bits is even.
mark	Always sets the parity bit to 1.
none	No parity bit used.
odd	Sets the parity bit to 1 if the number of 1 bits in the data sequence is even, or set to 1 if the number is odd.
space	Always sets the parity bit to 0.

Default Values

By default, the parity option is set to **none**.

Command History

Release 1.1	Command was introduced.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

Parity is the process used to detect whether characters have been altered during the data transmission process. Parity bits are appended to data frames to ensure that parity (whether it be odd or even) is maintained.

This command is not available for vAOS instances.

Usage Examples

The following example specifies **mark** parity for the console terminal session:

(config)**#line console 0**
(config-con 0)**#parity mark**

password *<password>*

Use the **password** command to configure the password (with optional encryption) required on the line session when security login is enabled (using the command *login on page 2031*). Use the **no** form of this command to remove a configured password. Variations of this command include:

password *<password>*
password md5 *<password>*

Syntax Description

<password>	Specifies the password for the line session using an alphanumeric character string (up to 16 characters).
md5	Specifies message digest 5 (MD5) as the encryption protocol to use when displaying the enable password during show commands. If the MD5 keyword is not used, encryption is not used when displaying the enable password during show commands.

Default Values

By default, there is no login password set for access to the unit.

Command History

Release 1.1	Command was introduced.
Release 6.1	Encryption was added.

Usage Examples

The following example enables the security login feature and specifies a password on the **CONSOLE** port:

(config)**#line console 0**
(config-con 0)**#login**
(config-con 0)**#password mypassword**

To provide extra security, AOS can encrypt the enable password when displaying the current configuration. For example, the following is a **show configuration** printout (password portion) with an unencrypted enable password (Adtran):

!
enable password Adtran
!

Alternately, the following is a **show configuration** printout (password portion) with an enable password of Adtran using md5 encryption:

!
enable password md5 encrypted 5aa5fbae7d01a90e79fb57705ce74676
!

speed *<rate>*

Use the **speed** command to specify the data rate for the **CONSOLE** port. This setting must match your VT100 terminal emulator or emulator software. Use the **no** form of this command to restore the default value.

Syntax Description

<rate>	Specifies rate of data transfer on the interface (2400; 4800; 9600; 19200; 38400; 57600; or 115200 bps).

Default Values

By default, the speed is set to **9600** bps.

Command History

Release 1.1	Command was introduced.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

This command is not available for vAOS instances.

Usage Examples

The following example configures the **CONSOLE** port for **19200** bps:

(config)**#line console 0**
(config-con 0)**#speed 19200**

stopbits *<value>*

Use the **stopbits** command to set the number of stopbits per character for a terminal session. This value must match the configuration of your VT100 terminal or terminal emulator software. The default is 1 stopbit per character. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the stopbits per character. Select from 1 or 2 stopbits per character.

Default Values

By default, the **stopbits** are set to **1**.

Command History

Release 1.1	Command was introduced.
Release R12.1.0	Command was made unavailable for virtual AOS (vAOS) instances.

Functional Notes

This command is not available for vAOS instances.

Usage Examples

The following example configures **2** stopbits per character for the console terminal session:

(config)**#line console 0**
(config-con 0)**#stopbits 2**

LINE (SSH) INTERFACE COMMAND SET

To activate the Line Secure Shell (SSH) Interface Configuration mode, enter the **line ssh** command specifying a SSH session(s) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#line ssh 0 4
(config-ssh0-4)#
```

You can select a single line by entering the **line ssh** command followed by the line number (0-4). For example:

```
>enable
#configure terminal
(config)#line ssh 2
(config-ssh2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

accounting commands begin on page 2039
authorization commands begin on page 2042
ip access-class <ipv4 acl name> in on page 2044
ip access-policy <ipv4 acp name> on page 2046
ipv6 access-class <ipv6 acl name> in on page 2048
line-timeout <value> on page 2050
login on page 2051
login authentication <listname> on page 2052
login local-userlist on page 2053

accounting commands <*level*> <*listname*>

Use the **accounting commands** command to assign authentication, authorization, and accounting (AAA) command accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA command accounting method list from the interface. Variations of this command include:

accounting commands <*level*> **default**
accounting commands <*level*> <*listname*>

Syntax Description

<*level*>	Specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
default	Applies the default AAA command accounting method list to the interface.
<*listname*>	Applies the specified AAA command accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA command accounting method lists are used to specify the types of information recorded when users access specified command levels. For more information about configuring command accounting lists, refer to the command *aaa accounting connection on page 1157*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA command accounting list **Accounting1** is applied to all Level **15** commands on all secure shell (SSH) lines:

(config)**#line ssh 0 4**
(config-ssh0-4)**#accounting commands 15 Accounting1**

accounting connection <*listname*>

Use the **accounting connection** command to assign authentication, authorization, and accounting (AAA) connection accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA connection accounting method list from the interface. Variations of this command include:

accounting connection default
accounting connection <*listname*>

Syntax Description

default	Applies the default AAA connection accounting method list to the interface.
<*listname*>	Applies the specified AAA connection accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA connection accounting method lists are used to specify the types of information recorded about outbound connections made from the AOS unit. For more information about configuring connection accounting lists, refer to the command *aaa accounting connection on page 1157*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA connection accounting list **AcctConn1** is applied to all secure shell (SSH) lines:

(config)**#line ssh 0 4**
(config-ssh0-4)**#accounting connection AcctConn1**

accounting exec <*listname*>

Use the **accounting exec** command to assign authentication, authorization, and accounting (AAA) executive accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA executive accounting method list from the interface. Variations of this command include:

accounting exec default
accounting exec <*listname*>

Syntax Description

default	Applies the default AAA connection accounting method list to the interface.
<*listname*>	Applies the specified AAA connection accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA executive accounting method lists are used to specify the types of information recorded about inbound connections made by connecting to the line interfaces and creating a terminal session. For more information about configuring executive accounting lists, refer to the command *aaa accounting exec on page 1160*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA executive accounting list **Inboundacct1** is applied to all secure shell (SSH) lines:

(config)**#line ssh 0 4**
(config-ssh0-4)**#accounting exec Inboundacct1**

authorization commands *<level> <listname>*

Use the **authorization commands** command to assign authentication, authorization, and accounting (AAA) command authorization method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA command authorization method list from the interface. Variations of this command include:

authorization commands *<level>* **default**
authorization commands *<level> <listname>*

Syntax Description

<level>	Specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
default	Applies the default AAA command authorization method list to the interface.
<listname>	Applies the specified AAA command authorization method list to the interface.

Default Values

By default, no AAA command authorization method list is applied to the line interface.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA command authorization method lists are used to allow or restrict the use of certain commands on a per-user basis. For more information about configuring command authorization lists, refer to the command *aaa authorization commands <level> on page 1176*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA command authorization list **Authorization1** is applied to all Level **15** commands on all secure shell (SSH) lines:

(config)**#line ssh 0 4**
(config-ssh0-4)**#authorization commands 15 Authorization1**

authorization exec *<listname>*

Use the **authorization exec** command to assign authentication, authorization, and accounting (AAA) Enable mode authorization method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA Enable mode authorization method list from the interface. Variations of this command include:

authorization exec default
authorization exec *<listname>*

Syntax Description

default	Applies the default AAA Enable mode authorization method list to the interface.
<listname>	Applies the specified AAA Enable mode authorization method list to the interface.

Default Values

By default, no AAA Enable mode authorization method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA Enable mode authorization method lists are used to allow or restrict user access to the privileged command line interface (CLI) mode (Enable mode). For more information about configuring Enable mode authorization lists, refer to the command *aaa authorization exec on page 1181*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA Enable mode authorization list **ExecList1** is applied to all secure shell (SSH) lines:

(config)**#line ssh 0 4**
(config-ssh0-4)**#authorization exec ExecList1**

ip access-class <*ipv4 acl name*> in

Use the **ip access-class in** command to restrict Internet Protocol version 4 (IPv4) secure shell (SSH) access using a configured access control list (ACL). Received IPv4 packets passed by the ACL will be allowed. Use the ACL configuration to deny hosts or entire networks or to permit specified IPv4 addresses. Use the **no** form of this command to disable this feature. Refer to *ip access-list standard <ipv4 acl name> on page 1346* and *ip access-list extended <ipv4 acl name> on page 1344* for more information about configuring ACLs. Variations of this command include:

ip access-class <*ipv4 acl name*> **in**
ip access-class <*ipv4 acl name*> **in any-vrf**
ip access-class <*ipv4 acl name*> **in vrf** <*name*>

Syntax Description

<*ipv4 acl name*>	Identifies the configured IPv4 ACL using an alphanumeric descriptor (all ACL descriptors are case sensitive).
any-vrf	Optional. Allows incoming connections from any virtual routing and forwarding (VRF) instance based on the parameters set in the ACL. Without this keyword, the ACL only applies to the default VRF and all SSH connections on nondefault VRFs will be ignored.
vrf <*name*>	Optional. Allows incoming connections from a specified VRF instance based on the parameters set in the access class list.

Default Values

By default, there are no configured IPv4 ACLs associated with SSH sessions.

Command History

Release 11.1	Command was introduced.
Release 16.1	Command was expanded to include the **any-vrf** parameter.
Release 18.2	Command was changed to include the **ip** parameter to accommodate Internet Protocol version 6 (IPv6) support for Adtran internetworking products only.
Release R10.1.0	Command was changed to include the **ip** parameter to accommodate Internet Protocol version 6 (IPv6) support for Adtran voice products.
Release R10.2.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

When using the **ip access-class in** command to associate an ACL with an SSH session, remember to duplicate the **ip access-class in** command for all configured SSH sessions 0 through 4. SSH access to the unit using a specific SSH session is not possible. Users will be assigned the first available SSH session.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example associates the IPv4 ACL **Trusted** (to allow SSH sessions from the 192.22.56.0 /24 network) with all SSH sessions (0 through 4) on all VRF instances:

Create the IPv4 ACL:

(config)**#ip access-list standard Trusted**
(config)**#permit 192.22.56.0 0.0.0.255**

Enter the line (SSH):

(config)**#line ssh 0 4**

Associate the ACL with the SSH session:

(config-ssh0-4)**#ip access-class Trusted in any-vrf**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the interface:

(config)**#line ssh 0 4**
(config-ssh0-4)**#ip access-policy PRIVATE**

ipv6 access-class <*ipv6 acl name*> in

Use the **ipv6 access-class in** command to restrict Internet Protocol version 6 (IPv6) secure shell (SSH) access using a configured access control list (ACL). Received IPv6 packets passed by the ACL will be allowed. Use the ACL configuration to deny hosts or entire networks or to permit specified IPv4 addresses. Use the **no** form of this command to disable this feature. Refer to *ipv6 access-list standard <ipv6 acl name> on page 1502* and *ipv6 access-list extended <ipv6 acl name> on page 1500* for more information about configuring ACLs. Variations of this command include:

ipv6 access-class <*ipv6 acl name*> **in**
ipv6 access-class <*ipv6 acl name*> **in any-vrf**
ipv6 access-class <*ipv6 acl name*> **in vrf** <*name*>

Syntax Description

<*ipv6 acl name*>	Identifies the configured IPv6 ACL using an alphanumeric descriptor (all ACL descriptors are case sensitive).
any-vrf	Optional. Allows incoming connections from any virtual routing and forwarding (VRF) instance based on the parameters set in the ACL. Without this keyword, the ACL only applies to the default VRF and all SSH connections on nondefault VRFs will be ignored.
vrf <*name*>	Optional. Allows incoming connections from a specified VRF instance based on the parameters set in the access class list.

Default Values

By default, there are no configured ACLs associated with SSH sessions.

Command History

Release 18.2	Command was introduced.
Release R10.2.0	Command was expanded to include the **vrf** <*name*> parameter.

Functional Notes

When using the **ipv6 access-class in** command to associate an ACL with an SSH session, remember to duplicate the **ipv6 access-class in** command for all configured SSH sessions 0 through 4. SSH access to the unit using a specific SSH session is not possible. Users will be assigned the first available SSH session.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example associates the IPv6 ACL **Trustedv6** (to allow SSH sessions from the **2001:DB8:3F::/64** network) with all SSH sessions (0 through 4) on all VRF instances:

Create the IPv6 ACL:

(config)**#ipv6 access-list extended Trustedv6**
(config-ext6-nacl)**#permit ipv6 2001:DB8:3F::/64 any**

Enter the line (SSH):

(config)**#line ssh 0 4**

Associate the ACL with the SSH session:

(config-ssh0-4)**#ipv6 access-class Trustedv6 in any-vrf**

line-timeout <*value*>

Use the **line-timeout** command to specify the number of minutes a line session may remain inactive before AOS terminates the session. Use the **no** form of this command to return to the default value. Variations of this command include:

line-timeout <*value*>
line-timeout <*value*> **any-activity**

Syntax Description

<*value*>	Specifies the number of minutes a line session may remain inactive before AOS terminates the session. Valid range: **0** to **35791**. Entering a **line-timeout** value of 0 disables the feature.
any-activity	Optional. Specifies that the SSH session does not time out until the specified value when the client is receiving or sending information with the AOS device.

Default Values

By default, the **line-timeout** is set to **15** minutes.

Command History

Release 11.1	Command was introduced.
Release R11.10.2	Command was expanded to include the **any-activity** parameter.

Functional Notes

The session timer is typically reset if data is sent from the client to the AOS device, but not if data is sent from the AOS device to the client. The optional **any-activity** parameter of this command prevents the session from timing out when the client is in a passive mode (only receiving data from the AOS device).

Usage Examples

The following example specifies a timeout of **2** minutes for all secure shell (SSH) sessions:

(config)**#line ssh 0 4**
(config-ssh0-4)**#line-timeout 2**

login

Use the **login** command to enable security login on the line session requiring the password configured using the **password** command. Use the **no** form of this command to disable the login feature.

Syntax Description

No subcommands.

Default Values

By default, secure login is disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password (**mypassword**) on all the available secure shell (SSH) sessions (0 through 4):

(config)**#line ssh 0 4**
(config-ssh0-4)**#login**
(config-ssh0-4)**#password mypassword**

login authentication <*listname*>

Use the **login authentication** command to apply the named authentication, authorization, and accounting (AAA) login method list to the line interface for authenticating users connecting to the interface. Use the **no** form of this command to remove the authentication method list from the interface.

Syntax Description

<*listname*>	Specifies the AAA login authentication method list to use for authentication.

Default Values

By default, no AAA login authentication method list is specified. If AAA is enabled (using the command *aaa on on page 1187*), but no login authentication method list is specified, the **default** login authentication method list is used. If the default list is used, but the default list has not been configured, secure shell (SSH) interfaces use the local user database for authentication.

Command History

Release 5.1	Command was introduced.

Functional Notes

AAA login authentication method lists are used to verify user logins on the line interface. For more information about configuring login authentication method lists, refer to the command *aaa authentication login on page 1169*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the AAA login authentication method list **AuthList1** is applied to all SSH lines:

(config)**#line ssh 0 4**
(config-ssh0-4)**#login authentication AuthList1**

login local-userlist

Use the **login local-userlist** command to check the local list of user names and passwords configured using the **username/password** Global Configuration command (refer to *username <username> password <password> on page 1887*).

> NOTE *All user properties assigned using the **username/password** command are valid when using the **login local-userlist** command.*

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example creates a local userlist and enables the security login feature:

(config)**#username my_user password my_password**
(config)**#line ssh 0**
(config-ssh0)**#login local-userlist**

When connecting to the unit, the following prompts are displayed:

User Access Login
Username: **my_user**
Password:
#

LINE (TELNET) INTERFACE COMMAND SET

To activate the Line (Telnet) Interface Configuration mode, enter the **line telnet** command specifying a Telnet session(s) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#line telnet 0 4
(config-telnet0-4)#
```

You can select a single line by entering the **line telnet** command followed by the line number (0-4). For example:

```
>enable
#configure terminal
(config)#line telnet 2
(config-telnet2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

accounting commands begin on page 2055
authorization commands begin on page 2058
ip access-class <ipv4 acl name> in on page 2060
ip access-policy <ipv4 acp name> on page 2062
ipv6 access-class <ipv6 acl name> in on page 2064
line-timeout <value> on page 2066
login on page 2067
login authentication <listname> on page 2068
login local-userlist on page 2069
password <password> on page 2070

accounting commands <*level*> <*listname*>

Use the **accounting commands** command to assign authentication, authorization, and accounting (AAA) command accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA command accounting method list from the interface. Variations of this command include:

accounting commands <*level*> **default**
accounting commands <*level*> <*listname*>

Syntax Description

<*level*>	Specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
default	Applies the default AAA command accounting method list to the interface.
<*listname*>	Applies the specified AAA command accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA command accounting method lists are used to specify the types of information recorded when users access specified command levels. For more information about configuring command accounting lists, refer to the command *aaa accounting connection on page 1157*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA command accounting list **Accounting1** is applied to all Level **15** commands on all Telnet lines:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting commands 15 Accounting1**

accounting connection <*listname*>

Use the **accounting connection** command to assign authentication, authorization, and accounting (AAA) connection accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA connection accounting method list from the interface. Variations of this command include:

accounting connection default
accounting connection <*listname*>

Syntax Description

default	Applies the default AAA connection accounting method list to the interface.
<*listname*>	Applies the specified AAA connection accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA connection accounting method lists are used to specify the types of information recorded about outbound connections made from the AOS unit. For more information about configuring connection accounting lists, refer to the command *aaa accounting connection on page 1157*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA connection accounting list **AcctConn1** is applied to all Telnet lines:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting connection AcctConn1**

accounting exec <*listname*>

Use the **accounting exec** command to assign authentication, authorization, and accounting (AAA) executive accounting method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA executive accounting method list from the interface. Variations of this command include:

accounting exec default
accounting exec <*listname*>

Syntax Description

default	Applies the default AAA connection accounting method list to the interface.
<*listname*>	Applies the specified AAA connection accounting method list to the interface.

Default Values

By default, no AAA command accounting method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA executive accounting method lists are used to specify the types of information recorded about inbound connections made by connecting to the line interfaces and creating a terminal session. For more information about configuring executive accounting lists, refer to the command *aaa accounting exec on page 1160*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA executive accounting list **Inboundacct1** is applied to all Telnet lines:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting exec Inboundacct1**

authorization commands *<level> <listname>*

Use the **authorization commands** command to assign authentication, authorization, and accounting (AAA) command authorization method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA command authorization method list from the interface. Variations of this command include:

authorization commands *<level>* **default**
authorization commands *<level> <listname>*

Syntax Description

<level>	Specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands.
default	Applies the default AAA command authorization method list to the interface.
<listname>	Applies the specified AAA command authorization method list to the interface.

Default Values

By default, no AAA command authorization method list is applied to the line interface.

Command History

Release 11.1	Command was introduced.

Functional Notes

AAA command authorization method lists are used to allow or restrict the use of certain commands on a per-user basis. For more information about configuring command authorization lists, refer to the command *aaa authorization commands <level> on page 1176*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA command authorization list **Authorization1** is applied to all Level **15** commands on all Telnet lines:

(config)**#line telnet 0 4**
(config-telnet0-4)**#authorization commands 15 Authorization1**

authorization exec <*listname*>

Use the **authorization exec** command to assign authentication, authorization, and accounting (AAA) Enable mode authorization method lists to line interfaces. You must first turn AAA on for this command to become available (using the command *aaa on on page 1187*). Use the **no** form of this command to remove the AAA Enable mode authorization method list from the interface. Variations of this command include:

authorization exec default
authorization exec <*listname*>

Syntax Description

default	Applies the default AAA Enable mode authorization method list to the interface.
<*listname*>	Applies the specified AAA Enable mode authorization method list to the interface.

Default Values

By default, no AAA Enable mode authorization method list is applied to the line interface.

Command History

Release 13.1	Command was introduced.

Functional Notes

AAA Enable mode authorization method lists are used to allow or restrict user access to the privileged command line interface (CLI) mode (Enable mode). For more information about configuring Enable mode authorization lists, refer to the command *aaa authorization exec on page 1181*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that AAA Enable mode authorization list **ExecList1** is applied to all Telnet lines:

(config)**#line telnet 0 4**
(config-telnet0-4)**#authorization exec ExecList1**

ip access-class *<ipv4 acl name>* in

Use the **ip access-class in** command to restrict Internet Protocol version 4 (IPv4) telnet access using a configured access control list (ACL). Received IPv4 packets passed by the ACL will be allowed. Use the ACL configuration to deny hosts or entire networks or to permit specified IPv4 addresses. Use the **no** form of this command to disable this feature. Refer to *ip access-list standard <ipv4 acl name> on page 1346* and *ip access-list extended <ipv4 acl name> on page 1344* for more information about configuring ACLs. Variations of this command include:

ip access-class *<ipv4 acl name>* **in**
ip access-class *<ipv4 acl name>* **in any-vrf**
ip access-class *<ipv4 acl name>* **in vrf** *<name>*

Syntax Description

<ipv4 acl name>	Identifies the configured IPv4 ACL using an alphanumeric descriptor (all ACL descriptors are case sensitive).
any-vrf	Optional. Allows incoming connections from any virtual routing and forwarding (VRF) instance based on the parameters set in the ACL. Without this keyword, the ACL only applies to the default VRF and all telnet connections on nondefault VRFs will be ignored.
vrf *<name>*	Optional. Allows incoming connections from a specified VRF instance based on the parameters set in the access class list.

Default Values

By default, there are no configured IPv4 ACLs associated with telnet sessions.

Command History

Release 11.1	Command was introduced.
Release 16.1	Command was expanded to include the **any-vrf** parameter.
Release 18.2	Command was changed to include the **ip** parameter to accommodate Internet Protocol version 6 (IPv6) support for Adtran internetworking products only.
Release R10.1.0	Command was changed to include the **ip** parameter to accommodate Internet Protocol version 6 (IPv6) support for Adtran voice products.
Release R10.2.0	Command was expanded to include the **vrf** *<name>* parameter.

Functional Notes

When using the **ip access-class in** command to associate an ACL with a telnet session, remember to duplicate the **ip access-class in** command for all configured telnet sessions 0 through 4. Telnet access to the unit using a specific telnet session is not possible. Users will be assigned the first available telnet session.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example associates the IPv4 ACL **Trusted** (to allow telnet nsessions from the 192.22.56.0 /24 network) with all telnet sessions (0 through 4) on all VRF instances:

Create the IPv4 ACL:

(config)**#ip access-list standard Trusted**
(config)**#permit 192.22.56.0 0.0.0.255**

Enter the line (Telnet):

(config)**#line telnet 0 4**

Associate the ACL with the SSH session:

(config-telnet0-4)**#ip access-class Trusted in any-vrf**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the interface:

(config)**#line telnet 0 4**
(config-telnet0-4)**#ip access-policy PRIVATE**

ipv6 access-class *<ipv6 acl name>* in

Use the **ipv6 access-class in** command to restrict Internet Protocol version 6 (IPv6) telnet access using a configured access control list (ACL). Received IPv6 packets passed by the ACL will be allowed. Use the ACL configuration to deny hosts or entire networks or to permit specified IPv4 addresses. Use the **no** form of this command to disable this feature. Refer to *ipv6 access-list standard <ipv6 acl name> on page 1502* and *ipv6 access-list extended <ipv6 acl name> on page 1500* for more information about configuring ACLs. Variations of this command include:

ipv6 access-class *<ipv6 acl name>* **in**
ipv6 access-class *<ipv6 acl name>* **in any-vrf**
ipv6 access-class *<ipv6 acl name>* **in vrf** *<name>*

Syntax Description

<ipv6 acl name>	Identifies the configured IPv6 ACL using an alphanumeric descriptor (all ACL descriptors are case sensitive).
any-vrf	Optional. Allows incoming connections from any virtual routing and forwarding (VRF) instance based on the parameters set in the ACL. Without this keyword, the ACL only applies to the default VRF and all telnet connections on nondefault VRFs will be ignored.
vrf *<name>*	Optional. Allows incoming connections from a specified VRF instance based on the parameters set in the access class list.

Default Values

By default, there are no configured ACLs associated with telnet sessions.

Command History

Release 18.2	Command was introduced.
Release R10.2.0	Command was expanded to include the **vrf** *<name>* parameter.

Functional Notes

When using the **ipv6 access-class in** command to associate an ACL with a telnet session, remember to duplicate the **ipv6 access-class in** command for all configured telnet sessions 0 through 4. Telnet access to the unit using a specific SSH session is not possible. Users will be assigned the first available telnet session.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example associates the IPv6 ACL **Trustedv6** (to allow telnet sessions from the **2001:DB8:3F::/64** network) with all telnet sessions (0 through 4) on all VRF instances:

Create the IPv6 ACL:

(config)**#ipv6 access-list extended Trustedv6**
(config-ext6-nacl)**#permit ipv6 2001:DB8:3F::/64 any**

Enter the line (telnet):

(config)**#line telnet 0 4**

Associate the ACL with the telnet session:

(config-telnet0-4)**#ipv6 access-class Trustedv6 in any-vrf**

line-timeout <*value*>

Use the **line-timeout** command to specify the number of minutes a line session may remain inactive before AOS terminates the session. Use the **no** form of this command to return to the default value. Variations of this command include:

line-timeout <*value*>
line-timeout <*value*> **any-activity**

Syntax Description

<*value*>	Specifies the number of minutes a line session may remain inactive before AOS terminates the session. Valid range: **0** to **35791**. Entering a **line-timeout** value of 0 disables the feature.
any-activity	Optional. Specifies that the SSH session does not time out until the specified value when the client is receiving or sending information with the AOS device.

Default Values

By default, the **line-timeout** is set to **15** minutes.

Command History

Release 11.1	Command was introduced.
Release R11.10.2	Command was expanded to include the **any-activity** parameter.

Functional Notes

The session timer is typically reset if data is sent from the client to the AOS device, but not if data is sent from the AOS device to the client. The optional **any-activity** parameter of this command prevents the session from timing out when the client is in a passive mode (only receiving data from the AOS device).

Usage Examples

The following example specifies a timeout of **2** minutes for all telnet sessions:

(config)**#line telnet 0**
(config-telnet0)**#line-timeout 2**

login

Use the **login** command to enable security login on the line session requiring the password configured using the **password** command. Use the **no** form of this command to disable the login feature.

Syntax Description

No subcommands.

Default Values

By default, secure login is disabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password on all the available Telnet sessions (0 through 4):

(config)**#line telnet 0 4**
(config-telnet0-4)**#login**
(config-telnet0-4)**#password mypassword**

login authentication <*listname*>

Use the **login authentication** command to apply the named authentication, authorization, and accounting (AAA) login method list to the line interface for authenticating users connecting to the interface. Use the **no** form of this command to remove the authentication method list from the interface.

Syntax Description

<*listname*>	Specifies the AAA login authentication method list to use for authentication.

Default Values

By default, no AAA login authentication method list is specified. If AAA is enabled (using the command *aaa on on page 1187*), but no login authentication method list is specified, the **default** login authentication method list is used. If the default list is used, but the default list has not been configured, Telnet interfaces use the local user database for authentication.

Command History

Release 5.1	Command was introduced.

Functional Notes

AAA login authentication method lists are used to verify user logins on the line interface. For more information about configuring login authentication method lists, refer to the command *aaa authentication login on page 1169*.

For more information about configuring AAA on your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the AAA login authentication method list **AuthList1** is applied to all Telnet lines:

(config)**#line telnet 0 4**
(config-telnet0-4)**#login authentication AuthList1**

login local-userlist

Use the **login local-userlist** command to enable security login for the terminal session requiring the user names and passwords configured using the **username/password** Global Configuration command. Use the **no** form of this command to disable the login local-userlist feature.

*All user properties assigned using the **username/password** command are valid when using the **login local-userlist** command.*

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example displays creating a local userlist and enabling the security login feature:

(config)**#username my_user password my_password**
(config)**#line telnet 0**
(config-telnet0)**#login local-userlist**

When connecting to the unit, the following prompts are displayed:

User Access Login
Username: **my_user**
Password:
Router#

password *<password>*

Use the **password** command to configure the password (with optional encryption) required on the line session when security login is enabled (using the **login** command). Use the **no** form of this command to remove a configured password. Variations of this command include:

password *<password>*
password md5 *<password>*

Syntax Description

<password>	Specifies the password for the line session using an alphanumeric character string (up to 16 characters).
md5	Optional. Specifies message digest 5 (MD5) as the encryption protocol to use when displaying the enable password during show commands. If the MD5 keyword is not used, encryption is not used when displaying the enable password during show commands.

Default Values

By default, there is no login password set for access to the unit.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password for the Telnet session 0:

(config)**#line telnet 0**
(config-telnet0)**#login**
(config-telnet0)**#password mypassword**

To provide extra security, AOS can encrypt the enable password when displaying the current configuration. For example, the following is a **show configuration** printout (password portion) with an unencrypted enable password (Adtran):

!
enable password Adtran
!

Alternately, the following is a **show configuration** printout (password portion) with an enable password of Adtran using md5 encryption:

!
enable password md5 encrypted 5aa5fbae7d01a90e79fb57705ce74676
!

PHYSICAL INTERFACE COMMAND SETS

This section includes the following command sets:

ADSL INTERFACE COMMAND SET

To activate the ADSL Interface Configuration mode, enter the **interface adsl** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface adsl 0/1
(config-adsl 0/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

interop-flag on page 2073
phy-flag on page 2074
retrain on page 2075
snr-margin on page 2076
training-mode on page 2077

interop-flag

This command is for future configuration and should not be modified.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.05	Command was introduced.

phy-flag

This command is for future configuration and should not be modified.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.05	Command was introduced.

retrain

Use the **retrain** command to force the modem to retrain.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example forces a modem retrain:

(config)**#interface adsl 0/1**
(config-adsl 0/1)**#retrain**

snr-margin

Use the **snr-margin** command to enable monitoring and set the minimum signal-to-noise ratio (SNR) during training and showtime. Use the **no** form of this command to disable monitoring. Variations of this command include:

snr-margin <*margin*>
snr-margin showtime monitor
snr-margin training monitor

Syntax Description

<*margin*>	Sets the minimum SNR margin value in dB. The range is from **1** to **15** dB.
showtime monitor	Enables margin monitoring to retrain the asymmetric digital subscriber line (ADSL) interface if the specified minimum margin is violated during showtime.
training monitor	Enables margin monitoring to retrain the ADSL interface if the specified minimum margin is violated during training.

Default Values

By default, SNR margin monitoring is disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example enables SNR margin monitoring during showtime with a minimum level of **7** dB:

(config)**#interface adsl 0/1**
(config-adsl 0/1)**#snr-margin showtime monitor 7**

training-mode

Use the **training-mode** command to configure the asymmetric digital subscriber line (ADSL) training mode. Use the **no** form of this command to disable a specific training mode. Variations of this command include:

training-mode ADSL2
training-mode ADSL2+
training-mode ADSL2+ANNEX-M
training-mode G.DMT
training-mode G.LITE
training-mode Multi-Mode
training-mode Multi-Mode-no-T1413
training-mode READSL2
training-mode T1.413

Syntax Description

ADSL2	Specifies International Telecommunication Union (ITU) G.992.3 mode.
ADSL2+	Specifies ITU G.992.5 mode.
ADSL2+ANNEX-M	Specifies ITU G.992.5 Annex M mode.
G.DMT	Specifies ANSI full-rate mode.
G.LITE	Specifies ANSI splitterless mode.
Multi-Mode	Specifies auto detect mode. When set to multi-mode, the ADSL interface attempts to train to the DSLAM using each of the supported training modes until a match is found.
Multi-Mode-no-T1413	Specifies auto detect mode without ANSI T1.413 capability.
READSL2	Specifies ITU G.992.3 Annex L mode.
T1.413	Specifies ANSI T1.413 mode.

Default Values

By default, the training mode is set to **Multi-Mode**.

Command History

Release 8.1	Command was introduced.
Release 13.1	Command was expanded to include the ITU G.992.5 Annex M mode.
Release A4.05	Command was expanded to include the **Multi-Mode-no-T1413** parameter.

Functional Notes

Some of the listed training modes (G.LITE, T1.413, ADSL2, ADSL2+, READSL2) are currently supported for ADSL over plain old telephone service (POTS) (Annex A) and are not valid for ADSL over integrated services digital network (ISDN) (Annex B) modules.

Usage Examples

The following example sets the training mode to **T1.413**:

(config)**#interface adsl 0/1**
(config-adsl 0/1)**#training-mode T1.413**

BRI INTERFACE COMMAND SET

To activate the BRI Interface Configuration mode, enter the **interface bri** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface bri 1/2
(config-bri 1/2)#
```

*The BRI number in the example above is shown as **bri 1/2**. This number is based on the interface's location (slot/port) and could vary depending on the unit's configuration. Use the **do show interfaces** command to determine the appropriate interface number.*

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

All other commands for this command set are described in this section in alphabetical order.

caller-id-override

Use the **caller-id-override** command to configure the unit to replace caller ID information with a user-specified number. Use the **no** form of this command to disable any caller ID overrides. Variations of this command include:

caller-id-override always <*number*>
caller-id-override if-no-cid <*number*>

Syntax Description

always <*number*>	Always forces replacement of the incoming caller ID number with the number given.
if-no-cid <*number*>	Replaces the incoming caller ID number with the number given only if there is no caller ID information available for the incoming call.

Default Values

By default, this command is disabled.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command forces a replacement of the incoming caller ID number with the number given. The received caller ID, if any, is discarded, and the given override number is used to connect the incoming call to a circuit of the same number.

Usage Examples

The following example configures the unit to always provide the given number as the caller ID number:

(config)**#interface bri 1/2**
(config-bri 1/2)**#caller-id-override always 5551000**

calling-party

Use the **calling-party** command to configure and control the basic rate interface (BRI) outgoing caller ID information. Use the **no** form of this command to disable this feature. Variations of this command include:

calling-party name <*name*>
calling-party number <*number*>
calling-party override always
calling-party override if-no-CID
calling-party presentation allowed
calling-party presentation not-available
calling-party presentation restricted
calling-party screening auto
calling-party screening network-provided

Syntax Description

name <*name*>	Configures the calling party name for the BRI.
number <*number*>	Configures the calling party number for the BRI.
override always	Enables the calling party to be replaced with the override number.
override if-no-CID	Enables the calling party to be replaced if caller ID number is not received.
presentation allowed	Enables the presentation of caller ID to always be allowed.
presentation not-available	Sets the calling party number to not available.
presentation restricted	Restricts the delivery on the caller ID information.
screening auto	Specifies that the calling party screening indicator is automatically determined.
screening network-provided	Specifies that the calling party screening indicator is provided by the network.

Default Values

By default, the command is disabled and the calling party screening indicator is set to **auto**.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was added to the BRI and the **screening auto** and **screening network-provided** parameters were added.

Usage Examples

The following example configures the calling party outgoing information to always provide the given number and name:

(config)**#interface bri 1/2**
(config-bri 1/2)**#calling-party override always**
(config-bri 1/2)**#calling-party presentation 555-8000**
(config-bri 1/2)**#calling-party name Company, Inc.**

clock source

Use the **clock source** command to configure the source timing used for the interface. Use the **no** form of this command to return to the default value. Variations of this command include:

clock source line
clock source system

Syntax Description

line	Configures the unit to recover clocking from the basic rate interface (BRI) circuit.
system	Configures the unit to provide clocking using the system clock.

Default Values

By default, the clock source is set to **system**.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example configures the unit to recover clocking from the circuit:

(config)**#interface bri 1/2**
(config-bri 1/2)**#clock source line**

isdn activation-timer <*value*>

Use the **isdn activation-timer** command to set the integrated services digital network (ISDN) T3 activation timer setting for the basic rate interface (BRI). This value is based upon the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendation 1.430. Use the **no** form of this command to return the timer to the default value.

Syntax Description

<*value*>	Specifies the ISDN activation timer in seconds. Valid range is **0** to **60** seconds. Using a value of **0** disables the timer.

Default Values

By default, the ISDN activation timer is set to **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example sets the ISDN activation timer to **20** seconds for the BRI:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn activation-timer 20**

isdn channel-flag

Use the **isdn channel-flag** to specify the integrated services digital network (ISDN) channel selection setting for the basic rate interface (BRI). Use the **no** form of this command to return to the default setting. Variations of this command include:

isdn channel-flag auto
isdn channel-flag exclusive
isdn channel-flag preferred

Syntax Description

auto	Specifies that the ISDN channel ID is automatically set to preferred or exclusive.
exclusive	Specifies that the ISDN channel ID is always set to exclusive.
preferred	Specifies that the ISDN channel ID is always set to preferred.

Default Values

By default, the ISDN channel ID is set to **auto**.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example specifies the ISDN channel selection for the interface as **exclusive**:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn channel-flag exclusive**

isdn disconnect progress-tone

Use the **isdn disconnect progress-tone** command to specify that calls are disconnected with a progress tone. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, call progress tones are not used.

Command History

Release R10.5.0	Command was introduced.

Usage Example

The following example enables the use of progress tones when calls are disconnected on the BRI:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn disconnect progress-tone**

isdn l2-disconnect <*value*>

Use the **isdn l2-disconnect** command to specify the disconnect delay of integrated services digital network (ISDN) Layer 2 functionality when there are no active calls. Use the **no** form of this command to disable the feature.

Syntax Description

<*value*>	Specifies the Layer 2 deactivation delay (in seconds). Valid range is **0** to **65535** seconds. Specifying a value of **0** disables the deactivation delay.

Default Values

By default, the Layer 2 disconnect feature is disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example configures the Layer 2 disconnect delay as **500** seconds:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn l2-disconnect 500**

isdn ldn

Use the **isdn ldn** command to specify the local directory numbers (LDNs) for the basic rate interface (BRI). This information should be supplied by your service provider. Use the **no** form of this command to remove a configured LDN. Variations of this command include:

isdn ldn1 *<ldn number>*
isdn ldn2 *<ldn number>*

*The BRI module requires all incoming calls to be directed to the LDN associated with the service profile identifier (SPID) programmed using the **isdn spid1** command. All calls to the LDN associated with SPID 2 will be rejected (unless part of a bonding call).*

Syntax Description

ldn1	Specifies the LDN associated with the SPID entered as **spid1**.
ldn2	Specifies the LDN associated with the SPID entered as **spid2**.
<ldn number>	Specifies the LDN assigned to the circuit by the service provider. The LDN is the number used by remote callers to dial into the integrated services digital network (ISDN) circuit.

Default Values

By default, there are no configured LDNs.

Command History

Release 12.1	Command was introduced.

Functional Notes

Inbound calls are not accepted on interfaces without programmed LDNs. LDNs can also be entered using the **isdn spid** command. The **isdn spid** and **isdn ldn** commands overwrite the existing programmed LDN; therefore, the latest LDN programmed takes precedence.

Usage Examples

The following example defines an LDN of **555-1111**:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn ldn1 5551111**

isdn line-termination

Use the **isdn line-termination** command to enable the integrated services digital network (ISDN) line termination resistor for the interface. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example enables the ISDN termination resistor on the BRI:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn line-termination**

isdn name-delivery

Use the **isdn name-delivery** command to enable the delivery of the name associated with the basic rate interface (BRI). Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, **isdn name-delivery** is disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example enables the delivery of calling party information on the BRI:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn name-delivery**

isdn overlap-receive

Use the **isdn overlap-receive** command to enable overlap receiving mode on the basic rate interface (BRI). Use the **no** form of this command to return to the default setting. Variations of this command include:

isdn overlap-receive timeout <*value*>
isdn overlap-receive digits-transferred <*value*>

Syntax Description

timeout <*value*>	Specifies how long the interface will attempt to match direct inward dialing (DID) digits received in INFO messages to entries in the voice dial-plan. If no matching entry is found, the interface will deliver the message when the timeout period expires. Valid range is **1** to **15** seconds.
digits-transferred <*value*>	Specifies how many DID digits the interface will collect before delivering the call. Valid range is **1** to **64** digits

Default Values

By default, **isdn overlap-receive** is disabled.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

When **isdn overlap-receive** is enabled, the interface will accept a SETUP message where the Called Party Number (CPN) information element is either missing or does not have enough DID digits. When more digits are received in subsequent INFO messages, the number is matched against entries in the voice dial-plan to determine when there are enough digits to deliver the call.

If no matching voice dial-plan entry is found, the interface will deliver the call when configuration the **isdn overlap-receive timeout** expires.

When **isdn overlap-receive did-length** is configured, no voice dial-plan look-up occurs. The interface will deliver the call as soon as the specified number of DID digits has been collected.

If at any time an INFO message is received with CPN information element containing **#** or a Sending Complete information element is received, the interface will deliver the call immediately.

Usage Examples

The following example enables overlap receiving with a timeout value of **7** seconds on the BRI:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn overlap-receiving timeout 7**

isdn setup enable

Use the **isdn setup enable** command to enable progress indicators in the integrated services digital network (ISDN) setup message and redirecting numbers for ISDN calls on the basic rate interface (BRI). The redirecting number is used to insert the caller's number when a call is diverted by a blind transfer or forward that both occurs on an ISDN trunk in local mode and proceeds out of an ISDN trunk. Use the **no** form of this command to disable this feature. Variations of this command include:

isdn setup enable called
isdn setup enable calling
isdn setup enable pi-1
isdn setup enable pi-3
isdn setup enable redirecting-number

Syntax Description

called	Enables the called number in ISDN setup messages.
calling	Enables the calling number in ISDN setup messages.
pi-1	Enables progress indicator 1 for ISDN setup messages. Progress indicator 1 indicates that the call is not end-to-end ISDN and further call progress information may be available in-band.
pi-3	Enables progress indicator 3 for ISDN setup messages. Progress indicator 3 indicates that the origination address is non-ISDN.
redirecting-number	Enables redirecting numbers for ISDN calls.

Default Values

By default, the called and calling numbers are included in ISDN setup messages.

Command History

Release A4.01	Command was introduced.
Release A4.03	Command was expanded to include the **redirecting-number** parameter.
Release R10.5.0	Command was expanded to include the BRI and the **called** and **calling** parameters.

Usage Examples

The following example enables redirecting numbers for ISDN calls on the BRI:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn setup enable redirecting-number**

isdn spid

Use the **isdn spid** command to specify the service profile identifiers (SPIDs) and the local directory numbers (LDNs) for the basic rate interface (BRI). This information should be supplied by your service provider. Use the **no** form of this command to remove a configured SPID. Variations of this command include:

isdn spid1 <*spid number*> <*ldn number*>
isdn spid2 <*spid number*> <*ldn number*>

*The BRI module requires all incoming calls to be directed to the LDN associated with the SPID programmed using the **isdn spid1** command. All calls to the LDN associated with SPID 2 will be rejected (unless part of a bonding call).*

Syntax Description

spid1	Specifies the primary SPID.
spid2	Specifies the secondary SPID.
<*spid number*>	Specifies the 8- to 14-digit number identifying your BRI line in the central office switch. A SPID is generally created using the area code and phone number associated with the line and a four-digit suffix. For example, the following SPIDs may be provided on a BRI line with phone numbers 555-1111 and 555-1112: SPID 1: 701 555 1111 0101 SPID 2: 701 555 1112 0101
<*ldn number*>	Optional. Specifies the LDN assigned to the circuit by the service provider. An LDN programmed using the **isdn spid1** command is automatically associated with SPID 1. An LDN programmed using the **isdn spid2** command is automatically associated with SPID 2. The LDN is the number used by remote callers to dial into the integrated services digital network (ISDN) circuit. Inbound calls are not accepted on interfaces without programmed LDNs. LDNs can also be entered using the **isdn ldn** command. The **isdn spid** and **isdn ldn** commands overwrite the existing programmed LDN; therefore, the latest LDN programmed takes precedence.

Default Values

By default, there are no configured SPIDs or LDNs.

Command History

Release 1.1	Command was introduced.

Functional Notes

AOS does not support “SPID-less” 5ESS signaling. SPIDs are required for all configured BRI endpoints using 5ESS signaling.

For European applications, a SPID is not necessary. Use the **isdn ldn** command to configure the LDN for European applications.

Usage Examples

The following example defines a SPID of **704 555 1111 0101** with an LDN of **555 1111**:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn spid1 70455511110101 5551111**

isdn static-tei <*value*>

Use the **isdn static-tei** command to configure a static integrated services digital network (ISDN) Layer 2 terminal endpoint identifier (TEI). Use the **no** form of this command to remove the TEI.

Syntax Description

<*value*>	Specifies the TEI. Valid range is **0** to **63**.

Default Values

By default, no static TEI exists.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example creates a static ISDN TEI of **5**:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn static-tei 5**

isdn switch-type

Use the **isdn switch-type** command to specify the integrated services digital network (ISDN) signaling type configured on the basic rate interface (BRI). The type of ISDN signaling implemented on the BRI does not always match the manufacturer of the central office switch. Use the **no** form of this command to return to the default value. Variations of this command include:

isdn switch-type basic-5ess
isdn switch-type basic-dms
isdn switch-type basic-net3
isdn switch-type basic-ni

Syntax Description

basic-5ess	Specifies Lucent/AT&T 5ESS signaling.
basic-dms	Specifies Nortel DMS-100 custom signaling.The **basic-dms** signaling type is not compatible with proprietary SL-1 DMS signaling.
basic-net3	Specifies Net3 Euro-ISDN signaling.
basic-ni	Specifies National ISDN-1 signaling.

Default Values

By default, the ISDN signaling is set to National ISDN-1 (**basic-ni**).

Command History

Release 1.1	Command was introduced.

Functional Notes

The **isdn switch-type** command specifies the type of ISDN signaling implemented on the BRI, not the manufacturer of the central office switch. It is quite possible to have a Lucent Central Office switch providing National ISDN signaling on the BRI.

Usage Examples

The following example configures a BRI for a circuit with Lucent 5ESS (custom) signaling:

(config)**#interface bri 1/2**
(config-bri 1/2)**#isdn switch-type basic-5ess**

loopback local

Use the **loopback local** command to enable a local loopback of the interface (towards the router). Use the **no** form of this command to disable the loopback. Variations of this command include:

loopback local all
loopback local b1
loopback local b2
loopback local both

Syntax Description

all	Loops the entire interface back towards the router (including the D-channel). With an active **loopback active all**, the established D-channel between the integrated services digital network (ISDN) module and the central office switch drops.
b1	Loops the data on B1 back towards the router. A B1 loopback does not disrupt D-channel signaling.
b2	Loops the data on B2 back towards the router. A B2 loopback does not disrupt D-channel signaling.
both	Loops the data on B1 and B2 back towards the router, but does not disrupt D-channel signaling.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables a B2 loopback of the basic rate interface (BRI) 1/2 interface:

(config)**#interface bri 1/2**
(config-bri 1/2)**#loopback local b2**

loopback network

Use the **loopback network** command to enable a loopback of the interface (towards the network). Use the **no** form of this command to disable the loopback. Variations of this command include:

loopback network b1
loopback network b2
loopback network both

Syntax Description

b1	Loops the data on B1 back towards the network. A B1 loopback does not disrupt D-channel signaling.
b2	Loops the data on B2 back towards the network. A B2 loopback does not disrupt D-channel signaling.
both	Loops the data on B1 and B2 back towards the network, but does not disrupt D-channel signaling.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables a B2 loopback of the basic rate interface (BRI) 1/2 interface:

(config)**#interface bri 1/2**
(config-bri 1/2)**#loopback network b2**

maintenance

Use the **maintenance** command to force a reset of the interface (initiating the SABME/UA process) or to reset the D-channel (by sending a RESTART message). Variations of this command include:

maintenance reset
maintenance restart-d

*The **maintenance** command disrupts data flow on the integrated services digital network (ISDN) interface. All active calls will drop when the reset or restart process begins.*

Syntax Description

reset	Forces a complete reset of the interface by initiating the SABME/UA process.
restart-d	Resets the D-channel by sending a Q.931 RESTART message to the central office switch.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example resets the basic rate interface (BRI) 1/2 interface:

(config)**#interface bri 1/2**
(config-bri 1/2)**#maintenance reset**

resource pool-member <*name*>

Use the **resource pool-member** command to assign the interface to a resource pool, making it a demand routing resource. Use the **no** form of this command to return to the default value. Variations of this command include:

resource pool-member <*name*>
resource pool-member <*name*> <*priority*>

Syntax Description

<*name*>	Specifies the name of the resource pool to which this interface is assigned.
<*priority*>	Optional. Specifies the priority value of using this interface versus other interfaces contained in the specified resource pool using a number **1** to **255**. Lower numbers indicate higher priority. Interfaces with the same priority are selected in alphabetical order by interface name.

Default Values

By default, the interface is not assigned to any resource pool.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures a basic rate interface (BRI) as a member of resource pool **MyPool**:

(config)**#interface bri 1/2**
(config-bri 1/2)**#resource pool-member MyPool**

role

Use the **role** command to configure the interface protocol to use on the basic rate interface (BRI). This setting controls the functional mode of the interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

role network
role user

Syntax Description

network	Sets the port to operate in network termination (NT) mode.
user	Sets the port to operate in terminal equipment (TE) mode.

Default Values

By default, the role is set to **network**.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was expanded to include the BRI.

Usage Examples

The following example configures the interface protocol as **user** on the BRI:

(config)**#interface bri 1/2**
(config-bri 1/2)**#role user**

system-timing

Use the **system-timing** command to configure the Rx clock as the primary or secondary timing source for the system. Use the **no** form of this command to disable this feature.Variations of this command include:

system-timing primary
system-timing secondary

Syntax Description

primary	Specifies the Rx clock as the primary timing source.
secondary	Specifies the Rx clock as the secondary timing source.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.
Release R10.5.0	Command was expanded to include the basic rate interface (BRI).

Usage Examples

The following example configures the BRI interface to provide its Rx clock as the primary timing source for the system:

(config)**#interface bri 1/2**
(config-bri 1/2)**#system timing primary**

test-call

Use the **test-call** command to initiate a test call on the basic rate interface (BRI) to test integrated services digital network (ISDN) connectivity without disrupting the primary interface for which the BRI interface is a backup. Use the **no** form of this command to disable this feature. Variations of this command include:

test-call answer
test-call dial <*number*>
test-call dial <*number*> **speed** [**56** | **64**]
test-call hangup
test-call hangup channels <*number*>

Syntax Description

answer	Places the unit in answer mode for test calls.
dial <*number*>	Specifies a test number to dial. No special characters are allowed. For example, **12125551212** is accepted, but **1-212-555-1212** and **1 (212) 555-1212** are not accepted.
speed [**56** | **64**]	Optional. Specifies the channel speed (in kilobytes per second) of the call. Valid speeds are **56** and **64**.
hangup	Terminates all test calls on all channels.
channels <*number*>	Optional. Specifies a single channel on which to terminate a test call. For a list of available channels, enter **test-call hangup channels ?** at the prompt.

Default Values

No default values are necessary for this command.

Command History

Release 18.1	Command was introduced.

Functional Notes

To successfully place a test call, a remote unit must be configured to answer the test call using the **test-call answer** command, and a separate local unit must be used to dial the test call number using the **test-call dial** <*number*> command.

Usage Examples

The following example places a test call over **bri 1/1** to **5555300**:

(config-bri 1/1)**#test-call dial 5555300**

2011.02.11 14:58:10 ISDN.INTERFACE BRI 1/1 Entering test-call mode.
2011.02.11 14:58:10 ISDN.INTERFACE BRI 1/1 Placing test-call to 5555300

CELLULAR INTERFACE COMMAND SET

To create a cellular interface and activate the Cellular Interface Configuration mode, enter the **interface cellular** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface cellular 1/1
(config-cellular 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

apn <name> on page 2106
cdma activate oma-dm on page 2107
cdma activate otasp on page 2108
cdma msl <number> on page 2109
custom-profile ha-shared-secret on page 2110
custom-profile home-address <ip address> on page 2111
custom-profile primary-ha-address <ip address> on page 2112
custom-profile secondary-ha-address <ip address> on page 2113
custom-profile username <username> on page 2114
match ani <template> substitute <template> on page 2115
reset on page 2117
resource pool-member <name> on page 2118
retry-throttling on page 2119
usb-id <value> on page 2120

apn <*name*>

Use the **apn** command to change the name of the access point associated with your universal serial bus (USB) cellular modem. Use the **no** version of this command to remove the name.

Syntax Description

<*name*>	Specifies the modem's access point name (APN) that is supplied by your service provider.

Default Values

By default, the APN is set to the name provided by the cellular service provider.

Command History

Release 18.2	Command was introduced.

Functional Notes

If you purchased your USB cellular modem in the Unites States, your APN is automatically set correctly. Adtran recommends that you do not change this setting. In countries other than the United States, where modems and cellular service are sold separately, the APN may not be defined. If the APN is not defined or incorrect, contact your service provider.

Usage Examples

In the following example, the APN is specified as **isp.cingular**:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#apn isp.cingular**

cdma activate oma-dm

Use the **cdma activate oma-dm** command to activate the cellular interface for connection to the Sprint wireless network.

Syntax Description

No subcommands.

Default Values

By default, the cellular interface is deactivated.

Command History

Release 17.4	Command was introduced.

Usage Examples

The following example activates cellular interface 1/1:

(config)**#interface cellular 1/1**
(config-cellular-1/1)**#cdma activate oma-dm**

cdma activate otasp

Use the **cdma activate otasp** command to activate the cellular interface for connection to the Verizon wireless network.

Syntax Description

No subcommands.

Default Values

By default, the cellular interface is disabled.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example activates cellular interface 1/1:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#cdma activate otasp**

cdma msl *<number>*

Use the **cdma msl** command to enter the 6-digit Sprint Master Subsidy Lock (MSL) code. Use the **no** form of this command to remove the code.

Syntax Description

<number>	Specifies the 6-digit Sprint MSL code.

Default Values

By default, no MSL code is activated.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example enters MSL code **526510** on cellular interface 1/1:

(config)**#interface cellular 1/1**
(config-cellular-1/1)**#cdma msl 526510**

custom-profile ha-shared-secret

Use the **custom-profile ha-shared-secret** command to specify the home agent shared secret for the cellular custom profile. Use the **no** form of this command to remove the shared secret from the custom profile configuration. Variations of this command include:

custom-profile ha-shared-secret ascii <*shared secret*>
custom-profile ha-shared-secret hexadecimal <*shared secret*>

Syntax Description

ascii <*shared secret*>	Specifies a plain text secret. Secret can be up to **16** characters in length.
hexadecimal <*shared secret*>	Specifies a hexadecimal secret. Secret can be up to **32** characters in length.

Default Values

By default, no custom profile is configured.

Command History

Release 17.5	Command was introduced.

Functional Notes

Cellular custom profile settings are useful for services that require manual activation or for services that allow remote access to private networks over the 3G network. For more information about custom profile settings, refer to the *3G CDMA NIM and the Cellular Interface* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates a plain text home agent shared secret (**sharedsecret**) for the custom profile:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#custom-profile ha-shared-secret ascii sharedsecret**

custom-profile home-address *<ip address>*

Use the **custom-profile home-address** command to specify the home address for the cellular custom profile. Use the **no** form of this command to remove the home address from the custom profile settings.

Syntax Description

<ip address>	Specifies the IP address of the home address. Enter IP addresses in dotted decimal notation (**XX.XX.XX.XX**).

Default Values

By default, no custom profile is configured.

Command History

Release 17.5	Command was introduced.

Functional Notes

Cellular custom profile settings are useful for services that require manual activation or for services that allow remote access to private networks over the 3G network. For more information about custom profile settings, refer to the *3G CDMA NIM and the Cellular Interface* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the home address for the custom profile:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#custom-profile home-address 192.168.1.1**

custom-profile primary-ha-address *<ip address>*

Use the **custom-profile primary-ha-address** command to specify the primary home agent IP address for the cellular custom profile. Use the **no** form of this command to remove the primary home agent IP address from the custom profile settings.

Syntax Description

<ip address>	Specifies the IP address of the primary home agent. Enter IP addresses in dotted decimal notation (**XX.XX.XX.XX**).

Default Values

By default, no custom profile is configured.

Command History

Release 17.5	Command was introduced.

Functional Notes

Cellular custom profile settings are useful for services that require manual activation or for services that allow remote access to private networks over the 3G network. For more information about custom profile settings, refer to the *3G CDMA NIM and the Cellular Interface* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the primary home agent IP address for the custom profile:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#custom-profile primary-ha-address 192.168.1.5**

custom-profile secondary-ha-address *<ip address>*

Use the **custom-profile secondary-ha-address** command to specify the secondary home agent IP address for the cellular custom profile. Use the **no** form of this command to remove the secondary home agent IP address from the custom profile settings.

Syntax Description

<ip address>	Specifies the IP address of the secondary home agent. Enter IP addresses in dotted decimal notation (**XX.XX.XX.XX**).

Default Values

By default, no custom profile is configured.

Command History

Release 17.5	Command was introduced.

Functional Notes

Cellular custom profile settings are useful for services that require manual activation or for services that allow remote access to private networks over the 3G network. For more information about custom profile settings, refer to the *3G CDMA NIM and the Cellular Interface* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the secondary home agent IP address for the custom profile:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#custom-profile secondary-ha-address 192.168.1.6**

custom-profile username <*username*>

Use the **custom-profile username** command to specify the username and password for the cellular custom profile. Use the **no** form of this command to remove the username and password from the custom profile settings. Variations of this command include:

custom-profile username <*username*>
custom-profile username <*username*> **password ascii** <*password*>
custom-profile username <*username*> **password hexadecimal** <*password*>

Syntax Description

username <*username*>	Specifies the user name for the custom profile. The user name is equivalent to network address identifier (NAI) user identification. User names can be up to **72** characters in length.
password ascii <*password*>	Specifies the plain text password. Passwords are equivalent to authentication, authorization, and accounting (AAA) shared secrets. Passwords can be up to **16** characters in length.
password hexadecimal <*password*>	Specifies the hexadecimal password. Passwords are equivalent to AAA shared secrets. Passwords can be up to **32** characters in length.

Default Values

By default, no custom profile is configured.

Command History

Release 17.5	Command was introduced.

Functional Notes

Cellular custom profile settings are useful for services that require manual activation or for services that allow remote access to private networks over the 3G network. For more information about custom profile settings, refer to the *3G CDMA NIM and the Cellular Interface* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the user name and plain text password for the custom profile:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#custom-profile username USERNAME password ascii PASSWORD**

match ani <*template*> substitute <*template*>

Use the **match ani substitute** command to configure automatic number identification (ANI) substitution for outbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

match ani <*template*> **substitute** <*template*>
match ani <*template*> **substitute** <*template*> **name** <*name*>

Syntax Description

ani <*template*>	Specifies the ANI information to be substituted. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the ANI information that is substituted for the original ANI information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
name <*name*>	Optional. Specifies the name associated with the ANI information. This option is only available on trunks that support ANI name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no ANI substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for ANI templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the ANI information from numbers **555-8111** to **555-8115** will be substituted by **555-8110** for outbound calls on interface 1/1:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#match ani 555-811[125] substitute 555-8110**

reset

Use the **reset** command to reboot the cellular network interface module (NIM).

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example reboots the NIM associated with cellular interface 1/1:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#reset**

resource pool-member <*name*>

Use the **resource pool-member** command to configure the cellular interface as a resource pool member for the demand interface to draw upon when connecting to the cellular network. Use the **no** form of this command to remove the interface from the resource pool. Variations of this command include:

resource pool-member <*name*>
resource pool-member <*name*> <*priority*>

Syntax Description

<*name*>	Specifies the resource pool to which the cellular interface is assigned.
<*priority*>	Optional. Specifies the priority this interface is given over other interfaces in the same pool. Range is **1** to **255**.

Default Values

By default, the cellular interface is not associated with any resource pools.

Command History

Release 17.2	Command was introduced.

Functional Notes

Lower priority values indicate a higher priority. Interfaces within the same resource pool with the same priority are selected as resources in alphabetical order by interface name.

Usage Examples

The following example configures interface **cellular 1/1** as a member of the **cellular** resource pool:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#resource pool-member cellular**

retry-throttling

Use the **retry-throttling** command to enable retry throttling. Use the **no** form of this command to disable retry throttling.

Syntax Description

No subcommands.

Default Values

In the Verizon cellular network, the retry throttle is enabled and cannot be disabled.

In the Sprint cellular network, the retry throttle is disabled by default but can be enabled by using this command.

Command History

Release 17.5	Command was introduced.

Functional Notes

When the retry throttle is enabled, it will disable the cellular interface for 15 minutes if a data call fails.

Usage Examples

The following example enables retry throttling:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#retry-throttling**

usb-id <*value*>

Use the **usb-id** command to specify which universal serial bus (USB) device the network interface module (NIM) will use. The USB ID is a combination of the vendor and product IDs. These values are displayed in the *show usb attached-devices on page 1061*.

Syntax Description

<*value*>	Specifies the identifying information for the USB device in the format <*vendor ID*> *:* <*product id*>. Each ID value is a 16-bit hexadecimal value, for example, **1234:ABCD**.

Default Values

No default values are necessary for this command.

Command History

Release R10.6.0	Command was introduced.

Functional Notes

The USB ID is a combination of the vendor and product ID. To view these values, enter the **show usb attached-devices** command as follows:

>**enable**
#show usb attached-devices
Device inserted in slot 1 on bus 0
Device Address: 1
Association: USB Cellular Interface /
Vendor: 0x1410 (Novatel Wireless Inc.)
Product: 0x6000 (Novatel Wireless CDMA)
Serial Number: 091165297381000
Device Class: 0x00 (NULL (PER INTERFACE))

The vendor ID (0x1410) and the product ID (0x6000) create the USB ID of **1410:6000**. This value is then entered as the USB ID using the **usb-id** command.

Usage Examples

The following example creates a USB ID of **1410:6000** on the cellular interface:

(config)**#interface cellular 1/1**
(config-cellular 1/1)**#usb-id 1410:6000**

DDS INTERFACE COMMAND SET

To activate the DDS Interface Configuration mode, enter the **interface dds** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface dds 1/1
(config-dds 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

clock rate on page 2122
clock source on page 2123
data-coding scrambled on page 2124
loopback on page 2125
remote-loopback on page 2126
snmp trap on page 2127
snmp trap link-status on page 2128

clock rate

Use the **clock rate** command to configure the data rate used as the operating speed for the interface. This rate should match the rate required by the digital data service (DDS) service provider. Use the **no** form of this command to return to the default value. Variations of this command include:

clock rate auto
clock rate bps56k
clock rate bps64k

Syntax Description

auto	Automatically detects the clock rate and sets to match.
bps56k	Sets the clock rate to **56** kbps.
bps64k	Sets the clock rate to **64** kbps.

Default Values

By default, the rate is set to **auto**.

Command History

Release 1.1	Command was introduced.

Functional Notes

When operating at 64 kbps (clear channel operation), the data terminal equipment (DTE) data sequences may mimic network loop maintenance functions and erroneously cause other network elements to activate loopbacks. Use the **data-coding scrambled** command to prevent such occurrences. Refer to *data-coding scrambled on page 2124* for related information.

Usage Examples

The following example configures the clock rate for **56** kbps operation:

(config)**#interface dds 1/1**
(config-dds 1/1)**#clock rate bps56k**

clock source

Use the **clock source** command to configure the source timing used for the interface. The clock specified using the **clock source** command is also the system master clock. Use the **no** form of this command to return to the default value. Variations of this command include:

clock source internal
clock source line

Syntax Description

internal	Configures the unit to provide clocking using the internal oscillator.
line	Configures the unit to recover clocking from the digital data service (DDS) circuit.

Default Values

By default, the clock source is set to **line**.

Command History

Release 1.1	Command was introduced.

Functional Notes

When operating on a DDS network, the clock source should be **line**. On a point-to-point private network, one unit must be **line** and the other **internal**.

Usage Examples

The following example configures the unit to recover clocking from the circuit:

(config)**#interface dds 1/1**
(config-dds 1/1)**#clock source line**

data-coding scrambled

Use the **data-coding scrambled** command to enable the digital data service (DDS) OS scrambler to combine user data with pattern data to ensure user data does not mirror standard DDS loop codes. The scrambler may only be used on 64 kbps circuits without Frame Relay signaling (clear channel). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the scrambler is disabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

When operating at 64 kbps (clear channel operation), there is a possibility the data terminal equipment (DTE) data sequences may mimic network loop maintenance functions and erroneously cause other network elements to activate loopbacks. Use the **data-coding scrambled** command to prevent such occurrences. Do not use this command if using Frame Relay or if using Point-to-Point Protocol (PPP) to another device other than an AOS product also running scrambled.

Usage Examples

The following example enables the DDS OS scrambler:

(config)**#interface dds 1/1**
(config-dds 1/1)**#data-coding scrambled**

loopback

Use the **loopback** command to initiate a specified loopback on the interface. Use the **no** form of this command to deactivate the loop. Variations of this command include:

loopback dte
loopback line
loopback remote

Syntax Description

dte	Initiates a loop to connect the transmit and receive path through the unit.
line	Initiates a loop of the digital data service (DDS) circuit toward the network by connecting the transmit path to the receive path.
remote	Transmits a DDS loop code over the circuit to the remote unit. In response, the remote unit should initiate a line loopback.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example activates a line loopback on the DDS interface:

(config)**#interface dds 1/1**
(config-dds 1/1)**#loopback line**

remote-loopback

Use the **remote-loopback** command to configure the interface to respond to loopbacks initiated by a remote unit (or the service provider). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables remote loopbacks on the digital data service (DDS) interface:

(config)**#interface dds 1/1**
(config-dds 1/1)**#remote-loopback**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP capability on the digital data service (DDS) interface:

(config)**#interface dds 1/1**
(config-dds 1/1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all supported interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the digital data service (DDS) interface:

(config)**#interface dds 1/1**
(config-dds 1/1)**#no snmp trap link-status**

DSX-1 INTERFACE COMMAND SET

To activate the DSX-1 Interface Configuration mode, enter the **interface t1** command (and specify the DSX-1 port) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface t1 1/2
(config-t1 1/2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

coding on page 2130
framing on page 2131
line-length <value> on page 2132
loopback network on page 2133
loopback remote line inband on page 2134
remote-loopback on page 2135
signaling-mode on page 2136
snmp trap link-status on page 2137
test-pattern on page 2138

coding

Use the **coding** command to configure the line coding for a DSX-1 physical interface. This setting must match the line coding supplied on the circuit by the PBX. Use the **no** form of this command to return to the default setting. Variations of this command include:

coding ami
coding b8zs

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
b8zs	Configures the line coding for bipolar eight zero substitution (B8ZS).

Default Values

By default, all DSX-1 interfaces are configured with **b8zs** line coding.

Command History

Release 1.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the DSX-1 circuit. A mismatch will result in line errors (e.g., bipolar violations (BPVs)).

Usage Examples

The following example configures the DSX-1 interface for **ami** line coding:

(config)**#interface t1 1/2**
(config-t1 1/2)**#coding ami**

framing

Use the **framing** command to configure the framing format for the DSX-1 interface. This parameter should match the framing format set on the external device. Use the **no** form of this command to return to the default value. Variations of this command include:

framing d4
framing esf

Syntax Description

d4	Specifies D4 superframe (SF) format.
esf	Specifies extended superframe (ESF) format.

Default Values

By default, the framing format is set to **esf**.

Command History

Release 1.1	Command was introduced.

Functional Notes

A frame is comprised of a single byte from each of the T1's timeslots; there are 24 timeslots on a single T1 circuit. Framing bits are used to separate the frames and indicate the order of information arriving at the receiving equipment. D4 and ESF are two methods of collecting and organizing frames over the circuit.

Usage Examples

The following example configures the DSX-1 interface for **d4** framing:

(config)**#interface t1 1/2**
(config-t1 1/2)**#framing d4**

line-length <*value*>

Use the **line-length** command to set the line build out (LBO) (in feet or dB) for the DSX-1 interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the LBO for the DSX-1 interface. Valid options include: **-7.5** dB or **0** to **655** feet. Use the -7.5 dB option for maximum attenuation.

Default Values

By default, the LBO is set to **0** feet.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **line-length** value represents the physical distance between DSX equipment (measured in cable length). Based on this setting, the AOS device increases signal strength to compensate for the distance the signal must travel. Valid distance ranges are listed below:

- 0 to 133 feet
- 134 to 265 feet
- 266 to 399 feet
- 400 to 533 feet
- 534 to 655 feet

Usage Examples

The following example configures the DSX-1 interface **line-length** for **300** feet:

(config)**#interface t1 1/2**
(config-t1 1/2)**#line-length 300**

loopback network

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback network line
loopback network payload

Syntax Description

line	Initiates a metallic loopback of the physical DSX-1 network interface.
payload	Initiates a loopback of the T1 framer (CSU portion) of the DSX-1 network interface.

Default Values

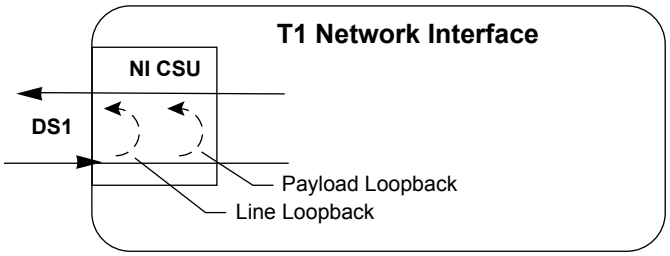
No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a payload loopback of the DSX-1 interface:

(config)**#interface t1 1/2**
(config-t1 1/2)**#loopback network payload**

loopback remote line inband

Use the **loopback remote line inband** command to send a loopback code to the remote unit to initiate a line loopback. Use the **no** form of this command to send a loopdown code to the remote unit to deactivate the loopback.

Syntax Description

inband	Uses the inband channel to initiate a full 1.544 Mbps physical (metallic) loopback of the signal received by the remote unit from the network.

Default Values

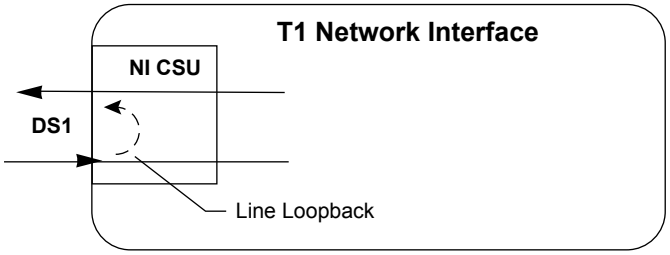
No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Functional Notes

A remote loopback can only be issued if a cross connect does not exist on the interface and if the signaling mode is set to **none**. The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a remote line loopback using the inband channel:

(config)**#interface t1 1/2**
(config-t1 1/2)**#loopback remote line inband**

remote-loopback

Use the **remote-loopback** command to configure the interface to respond to loopbacks initiated by a remote unit (or the service provider). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables remote loopbacks on the DSX-1 interface:

(config)**#interface t1 1/2**
(config-t1 1/2)**#remote-loopback**

signaling-mode

Use the **signaling-mode** command to configure the signaling type (robbed-bit for voice or clear channel for data) for the level zero digital signals (DS0s) mapped to the DSX-1 port. Use the **no** form of this command to return to the default setting. Variations of this command include:

signaling-mode message-oriented
signaling-mode none
signaling-mode robbed-bit

Syntax Description

message-oriented	Specifies clear channel signaling on Channel 24 only. Use this signaling type with QSIG installations.
none	Specifies clear channel signaling on all 24 DS0s. Use this signaling type with data-only or primary rate interface (PRI) DSX-1 installations.
robbed-bit	Specifies robbed bit signaling on all DS0s. Use this signaling type for voice-only DSX-1 applications.

Default Values

By default, the signaling mode is set to **robbed-bit**.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the DSX-1 port for PRI compatibility:

(config)**#interface t1 1/2**
(config-t1 1/2)**#signaling-mode none**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the DSX-1 interface:

(config)**#interface t1 1/2**
(config-t1 1/2)**#no snmp trap link-status**

test-pattern

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation. Variations of this command include:

test-pattern ones
test-pattern zeros

Syntax Description

ones	Generates a test pattern of continuous ones.
zeros	Generates a test pattern of continuous zeros.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example activates the pattern generator for a stream of continuous ones:

(config)**#interface t1 1/2**
(config-t1 1/2)**#test-pattern ones**

E1 INTERFACE COMMAND SET

To activate the E1 Interface Configuration mode, enter the **interface e1** command (and specify the E1 port) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface e1 1/1
(config-e1 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

clock source on page 2140
coding on page 2141
framing crc4 on page 2142
loop-alarm-detect on page 2143
loopback network on page 2144
loopback remote v54 on page 2145
remote-loopback on page 2146
sa4tx-bit <value> on page 2147
snmp trap line-status on page 2148
snmp trap link-status on page 2149
snmp trap threshold-reached on page 2150
system-timing on page 2151
tdm-group <number> on page 2152
test-pattern on page 2153
timing-domain <domain> on page 2154
ts16 on page 2155

clock source

Use the **clock source** command to configure the source timing used for the interface. Use the **no** form of this command to return to the default value. Variations of this command include:

clock source internal
clock source line
clock source system
clock source through

Syntax Description

internal	Configures the unit to provide clocking using the internal oscillator.
line	Configures the unit to recover clocking from the E1 circuit.
system	Configures the unit to provide clocking from the chassis selection.
through	Configures the unit to recover clocking from the circuit connected to the G.703 interface.

Default Values

By default, the unit is configured to recover clocking from the primary circuit.

Command History

Release 5.1	Command was introduced.
Release A2	Command was expanded to include the **system** parameter.

Functional Notes

When operating on a circuit that is providing timing, setting the **clock source** to **line** can avoid errors, such as clock slip seconds (CSS).

Usage Examples

The following example configures the unit to recover clocking from the primary circuit:

(config)**#interface e1 1/1**
(config-e1 1/1)**#clock source line**

coding

Use the **coding** command to configure the line coding for the E1 physical interface. This setting must match the line coding supplied on the circuit by the service provider. Use the **no** form of this command to return to the default setting. Variations of this command include:

coding ami
coding hdb3

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
hdb3	Configures the line coding for high-density bipolar 3 (HDB3).

Default Values

By default, all E1 interfaces are configured with **hdb3** line coding.

Command History

Release 5.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the E1 circuit. A mismatch will result in line errors (e.g., bipolar violations (BPVs)).

Usage Examples

The following example configures the E1 interface for **ami** line coding:

(config)**#interface e1 1/1**
(config-e1 1/1)**#coding ami**

framing crc4

Use the **framing crc4** command to configure the framing format for the E1 interface. This parameter should match the framing format provided by the service provider or external device. Use the **no** form of this command to return to the default value.

Syntax Description

crc4	Enables CRC4 bits to be transmitted in the outgoing data stream. Also, the received signal is checked for CRC4 errors.

Default Values

By default, CRC4 is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The framing value must match the configuration of the E1 circuit. A mismatch will result in a loss of frame alarm.

Usage Examples

The following example configures the E1 interface for CRC4 framing:

(config)**#interface e1 1/1**
(config-e1 1/1)**#framing crc4**

loop-alarm-detect

The **loop-alarm-detect** command enables detection of a loop alarm on the E1 interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command enables the detection of a loopback alarm. This alarm works in conjunction with the **sa4tx-bit** command setting. The loopback condition is detected by comparing the transmitted **sa4tx-bit** value to the received Sa4 bit value. If the bits match, a loopback is assumed. This detection method only works with a network in which the far end is transmitting the opposite value for Sa4.

Usage Examples

The following example enables detection of a loop alarm on the E1 interface:

(config)**#interface e1 1/1**
(config-e1 1/1)**#loop-alarm-detect**

loopback network

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback network line
loopback network payload

Syntax Description

line	Initiates a metallic loopback of the physical E1 network interface.
payload	Initiates a loopback of the E1 framer (CSU) portion of the E1 network interface.

Default Values

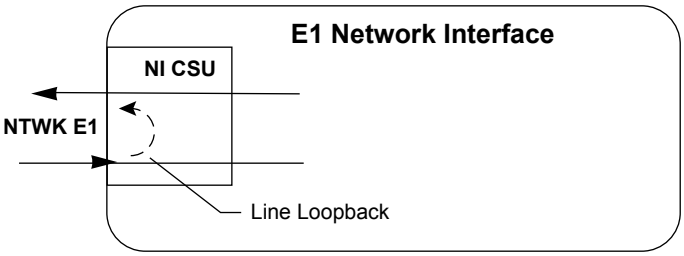
No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

The following diagram depicts a line loopback.



Usage Examples

The following example initiates a line loopback of the E1 interface:

(config)**#interface e1 1/1**
(config-e1 1/1)**#loopback network line**

loopback remote v54

The **loopback remote v54** command initiates an E1 remote loopback test (with a V.54 loopback pattern). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command causes a V.54 inband loop code to be sent in the payload towards the far end.

Usage Examples

The following example sends a V.54 inband loop code to the far end:

(config)**#interface e1 1/1**
(config-e1 1/1)**#loopback remote v54**

remote-loopback

Use the **remote-loopback** command to configure the interface to respond to loopbacks initiated by a remote unit (or the service provider). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Command History

Release 1.1	Command was introduced.

Functional Notes

This controls the acceptance of any remote loopback requests. When enabled, remote loopbacks are detected and cause a loopback to be applied. When disabled, remote loopbacks are ignored.

Usage Examples

The following example enables remote loopbacks on the E1 interface:

(config)**#interface e1 1/1**
(config-e1 1/1)**#remote-loopback**

sa4tx-bit <*value*>

The **sa4tx-bit** command selects the Tx value of Sa4 in this E1 interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies a **0** or a **1** for the transmit value of the SA4 bit on the E1.

Default Values

The default value for this command is **1**.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command assigns a value to the Tx spare bit in position 4. The odd-numbered frames of TS0 are not used for frame alignment. Bits in position 4 through 8 are called spare bits. Values of 0 or 1 are accepted.

TS0 odd frame

Bit position	1	2	3	4	5	6	7	8
Bit use	0	1	RAI = 1	S	S	S	S	S

Usage Examples

The following example sets the Tx value of Sa4 to **0**:

(config)**#interface e1 1/1**
(config-e1 1/1)**#sa4tx-bit 0**

snmp trap line-status

Use the **snmp trap line-status** command to control the Simple Network Management Protocol (SNMP) variable dsx1LineStatusChangeTrapEnable (RFC 2495) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the dsx1LineStatusChangeTrapEnable object identifier (OID) is set to enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 11.1	Command was introduced.

Functional Notes

The **snmp trap line-status** command is used to control the RFC 2495 dsx1LineStatusChangeTrapEnable OID (OID number 1.3.6.1.2.1.10.18.6.1.17.0).

Usage Examples

The following example disables the line-status trap on the T1 interface:

(config)**#interface e1 1/1**
(config-t1 1/1)**#no snmp trap line-status**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the E1 interface:

(config)**#interface e1 1/1**
(config-e1 1/1)**#no snmp trap link-status**

snmp trap threshold-reached

Use the **snmp trap threshold-reached** command to control the Simple Network Management Protocol (SNMP) variable adGenAOSDs1ThresholdReached (adGenAOSDs1-Ext MIB) to enable the interface to send SNMP traps when a DS1 performance counter threshold is reached. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the adGenAOSDs1ThresholdReached object identifier (OID) is disabled for all interfaces.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example disables SNMP threshold reached trap on the E1 interface:

(config)**#interface e1 1/1**
(config-e1 1/1)**#no snmp trap threshold-reached**

system-timing

Use the **system-timing** command to configure the system timing to use the E1 interface as the system clock source. Use the **no** form of this command to return to the default value. Variations of this command include:

system-timing primary
system-timing secondary

Syntax Description

primary	Configures the unit to use the E1 interface as the source of the primary system clock.
secondary	Configures the unit to use the E1 interface as the source of the secondary system clock.

Default Values

By default, the unit is configured to recover clocking from the primary circuit.

Command History

Release A2	Command was introduced.

Usage Examples

The following example configures the unit to use the E1 interface as the primary system timing source:

(config)**#interface e1 1/1**
(config-e1 1/1)**#system-timing primary**

tdm-group <*number*>

Use the **tdm-group** command to create a group of contiguous channels on this interface to be used during the **cross-connect** process. Use the **no** form of this command to remove configured time division multiplexing (TDM) groups. Refer to *cross-connect on page 76* for related information. Variations of this command include:

tdm-group <*number*> **timeslots** <*value*>
tdm-group <*number*> **timeslots** <*value*> **speed [56 | 64]**

*Changing **tdm-group** settings could result in service interruption.*

Syntax Description

<*number*>	Identifies the created TDM group. Valid range is **1** to **255**.
timeslots <*value*>	Specifies the channels to be used in the TDM group. Valid range is **1** to **31**. The timeslot value can be entered as a single number representing one of the 31 E1 channel timeslots or as a contiguous group of channels. (For example, **1-10** specifies the first 10 channels of the E1.)
speed [56 | 64]	Optional. Specifies the individual channel rate on the E1 interface to be 56 or 64 kbps. The default speed is 64 kbps. 56 kbps operation is not available on all E1 interfaces. Refer to the quick start guide provided with your E1 module to determine whether 56 kbps is valid.

Default Values

By default, there are no configured TDM groups.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example creates a TDM group (labeled **5**) of 10 channels at 64 kbps each:

(config)**#interface e1 1/1**
(config-e1 1/1)**#tdm-group 5 timeslots 1-10 speed 64**

test-pattern

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation. Variations of this command include:

test-pattern clear
test-pattern errors
test-pattern insert
test-pattern ones
test-pattern p215
test-pattern p220
test-pattern p511
test-pattern qrss
test-pattern zeros

Syntax Description

clear	Clears the test pattern error count.
errors	Displays the test pattern error count.
insert	Inserts an error into the currently active test pattern.
ones	Generates test pattern of continuous ones.
p215	Generates a pseudorandom test pattern sequence based on a 15-bit shift register.
p220	Generates a pseudorandom test pattern sequence based on a 20-bit shift register.
p511	Generates a test pattern of repeating ones and zeros.
qrss	Generates a test pattern of random ones and zeros.
zeros	Generates test pattern of continuous zeros.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example activates the pattern generator for a stream of continuous ones:

(config)**#interface e1 1/1**
(config-e1 1/1)**#test-pattern ones**

timing-domain <*domain*>

Use the **timing-domain** command to assign the interface to a system-wide voice timing domain. Use the **no** form of this command to return to the default.

Syntax Description

<*domain*>	Assigns the interface to a system-wide timing domain. Valid domains are **1** and **2**.

Default Values

By default, interfaces are assigned to timing domain **1**.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example assigns the interface to timing domain **2**:

(config)**#interface e1 1/1**
(config-e1 1/1)**#timing-domain 2**

ts16

Use the **ts16** command to enable timeslot 16 multiframe to be checked on the receive signal. Use the **no** form of this command to disable timeslot 16.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

If timeslot 16 is used on the incoming E1, do not map timeslot 16 using the **tdm-group** command. By default, all timeslots not physically mapped using the **tdm-group** command are passed through to the G.703 interface. Leaving timeslot 16 unmapped makes it available for multiframe signaling by the connected E1 device.

Usage Examples

The following example enables timeslot 16 multiframing:

(config)**#interface e1 1/1**
(config-e1 1/1)**#ts16**

ETHERNET INTERFACE COMMAND SET

There are multiple types of Ethernet interfaces associated with AOS:

- Basic Ethernet interfaces (e.g., eth 0/1)
- Gigabit Ethernet interfaces (e.g., giga-eth 0/3)
- Gigabit Ethernet subinterfaces associated with Layer 3 services (eg., giga-eth 0/1.1)
- Ethernet subinterfaces associated with a virtual local area network (VLAN) (e.g., eth 0/1.1)
- Ethernet subinterfaces associated with Layer 3 services (eg., eth 0/1.1)
- Switchport interfaces which are only available on specific platforms (e.g., swx 0/1)
- Gigabit switchport interfaces which are only available on specific platforms (e.g., giga-swx 0/1)
- 10 gigabit switchport interfaces which are only available on specific platforms (e.g., xgiga-swx 1/1)

Not all platforms have Ethernet subinterfaces, Gigabit Ethernet, switchport, or gigabit switchport interfaces available. To see if your unit has this capability, type ***show interfaces*** *at the enable prompt.*

To activate the basic Ethernet Interface Configuration mode, enter the **interface ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface ethernet 0/1
(config-eth 0/1)#
```

To activate the Ethernet Subinterface Configuration mode, enter the **interface ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface ethernet 0/1.1
(config-eth 0/1.1)#
```

To activate the Ethernet Subinterface Configuration mode for Layer 3 services, enter the **interface ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface ethernet 0/1.1
(config-eth 0/1.1)#
```


To activate the Gigabit Ethernet Interface Configuration mode, enter the **interface gigabit-ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface gigabit-ethernet 0/3
(config-giga-eth 0/3)#
```

To activate the Gigabit Ethernet Subinterface Configuration mode, enter the **interface gigabit-ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface gigabit-ethernet 0/3.1
(config-giga-eth 0/3.1)#
```

To activate the Gigabit Switchport Interface Configuration mode, enter the **interface gigabit-switchport** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface gigabit-switchport 0/3
(config-giga-swx 0/3)#
```

To activate the Switchport Interface Configuration mode, enter the **interface switchport** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface switchport 0/1
(config-swx 0/1)#
```

To activate the Ethernet Configuration mode for a range of Ethernet interfaces, enter the **interface range** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface range ethernet 0/1, 0/8
(config-eth 0/1, 0/8)#
```

To activate the 10 Gigabit Switchport Interface Configuration mode, enter the **interface xgigabit-switchport** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface xgigabit-switchport 1/1
(config-xgiga-swx 1/1)#
```

*Not all Ethernet commands apply to all Ethernet types. Use the **?** command to display a list of valid commands. For example:*

*>**enable***
*Password:**xxxxx***
#config term
*(config)#**interface ethernet 0/1***
*(config-eth 0/1)#**?***

alias	*- A text name assigned by an SNMP NMS*
arp	*- Set ARP commands*
awcp	*- Enables Adtran Wireless Control Protocol on this interface*
bandwidth	*- Set bandwidth parameter*
etc.	

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

arp arpa on page 2161
awcp on page 2162
bandwidth <value> on page 2163
bridge-group <number> on page 2165
bridge-group <number> vlan-transparent on page 2166
ce-vlan-id <vlan id> on page 2167
channel-group <number> mode on on page 2168
connect evc <name> on page 2169
dynamic-dns on page 2170
egress-queue on page 2172
encapsulation 802.1q on page 2173
ethernet-cfm down on page 2174
ethernet-cfm mep on page 2175

arp arpa

Use the **arp arpa** command to set ARPA as the standard Address Resolution Protocol (ARP) on this interface. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

The default for this command is **arpa**.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example enables standard ARP for the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#arp arpa**

awcp

Use the **awcp** command to enable Adtran Wireless Control Protocol (AWCP) on this interface. The AWCP is an Adtran proprietary protocol used by an access controller (AC) to communicate with an access point (AP). Use the **no** form of this command to disable AWCP for this interface.

Syntax Description

No subcommands.

Default Values

By default, AWCP is enabled on the interface.

Command History

Release 15.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

When the global-level command **dot11ap access-point-controller** (refer to *dot11ap access-point-control on page 1268* for more information) is enabled, the AWCP function can be disabled on a specific interface by using the **no** form of this command from the desired interface. When the global-level command **dot11ap access-point-controller** is disabled, it overrides the **awcp** command setting for the interface.

Usage Examples

The following example disables AWCP on Ethernet interface 0/1:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#no awcp**

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view default value, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 2272*) to adjust the bandwidth appropriately for QoS configurations.

When configuring QoS for an Ethernet or VLAN interface, the interface **traffic-shape rate** command can be used to configure traffic shaping without applying a QoS map. If traffic shaping is applied to the same interface that will also have a QoS map applied to it, the amount of bandwidth available for the QoS policy is reduced to the value set with the **traffic-shape rate** command (*page 2348*). This value should be set to match the upload speed of the circuit. For example, under normal circumstances, an Ethernet interface can negotiate to 100 Mbps. However, the throughput of the upstream equipment is usually significantly less than the negotiated rate. The **traffic-shape rate** command is used to define the limit of when QoS policies containing the commands *bandwidth on page 4466* or *priority on page 4481* should be enforced according to the upload speed of the circuit. If the **bandwidth** <*value*> command is also entered on the same IP interface as the **traffic-shape rate** command, it will overwrite the value of the **traffic-shape rate** command for QoS purposes. It is not recommended to use the **bandwidth** <*value*> command for QoS. Instead, use the **max-reserved-bandwidth** command (*page 2272*) to adjust the bandwidth appropriately because the **traffic-shape rate** command is required for QoS to function properly on VLAN and Ethernet WAN IP interfaces.

Usage Examples

The following example sets bandwidth of the Ethernet 0/1 interface to 10 Mbps:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#bandwidth 10000**

bridge-group *<number>*

Use the **bridge-group** command to assign an interface to the specified bridge group. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<number>	Specifies the bridge group (by number) to which to assign this interface. Range is **1** to **255**.

Default Values

By default, there are no configured bridge groups.

Command History

Release 1.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (e.g., Ethernet to T1 bridge, Ethernet to Frame Relay subinterface).

Usage Examples

The following example assigns the Ethernet interface to bridge-group **17**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#bridge-group 17**

bridge-group <*number*> vlan-transparent

Use the **bridge-group vlan-transparent** command to prevent an interface from removing the virtual local area network (VLAN) tag. Use the **no** form of this command to allow the interface to remove the VLAN tag from the packet.

*The **bridge-group vlan-transparent** command is not a global command. The command must be applied on all interfaces of the bridge group.*

Syntax Description

<number>	Specifies the bridge group number. Valid range is **1** to **255**.

Default Values

By default, VLAN tags are removed from the data.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the high level data link control (HDLC) interface and Frame Relay subinterface.

Usage Examples

The following example removes the VLAN tags from the packets on the Ethernet interface 0/1:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#bridge-group 1 vlan-transparent**

ce-vlan-id <*vlan id*>

Use the **ce-vlan-id** command to set a customer-edge (CE) virtual local area network (VLAN) ID for Layer 3 service subinterfaces used as the Metro Ethernet network (MEN) port. Use the **no** form of this command to remove the CE VLAN ID configuration from the subinterface. Variations of this command include:

ce-vlan-id <*vlan id*>
ce-vlan-id <*vlan id*> **untagged**

Syntax Description

<*vlan id*>	Specifies a valid CE VLAN interface ID number. Range is **1** to **4095**.
untagged	Optional. Specifies that all untagged packets are identified with this subinterface.

Default Values

By default, all Layer 3 service subinterface traffic is unspecified, which prevents the subinterface from becoming active.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example configures a CE VLAN of **100** for the Gigabit Ethernet subinterface 0/1.1:

(config)**#interface gigabit-ethernet 0/1.1**
(config-giga-eth 0/1.1)**#ce-vlan-id 100**

channel-group <*number*> mode on

Use the **channel-group mode on** command to statically add the interface to a channel group. To remove an interface from a channel group, use the **no** form of this command.

Syntax Description

<*number*>	Specifies the channel-group number. Range is **1** to **6**.

Default Values

By default, the interface is not part of a channel group.

Command History

Release 5.1	Command was introduced.

Functional Notes

There can be up to six channel groups with 2 to 8 interfaces per group. Dynamic protocols are not yet supported (only static). A physical interface can be a member of only one channel group.

Usage Examples

The following example adds the Ethernet 0/1 interface to channel group **1**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#channel-group 1 mode on**
(config-eth 0/1)#

connect evc *<name>*

Use the **connect evc** command to associate the Ethernet virtual connection (EVC) with the subinterface for Layer 3 Metro Ethernet network (MEN) to CPU communication. Use the **no** form of this command to remove the connection.

Syntax Description

<name>	Specifies the EVC to which the matching traffic is mapped.

Default Values

By default, no EVC components are connected to the subinterface.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

The EVC's connected MEN port must match the parent interface of the Layer 3 subinterface for the subinterface to be active. This command is required if the parent interface is a network-to-network interface (NNI) and will not function if the parent interface is a user network interface (UNI).

Usage Examples

The following example specifies that EVC **CustomerSVC** is associated with Gigabit Ethernet subinterface 1/1.1:

(config)**#interface gigabit-ethernet 1/1.1**
(config-giga-eth-1/1.1)**#connect evc CustomerSVC**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies the user name.
<*password*>	Specifies the password.
	Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user's name **user**, and password **pass**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#dynamic-dns dyndns-custom host user pass**

egress-queue

Use the **egress-queue** command to specify the output queue used by the Ethernet virtual connection (EVC) for traffic egressing this Layer 3 interface towards the user network interface (UNI). Use the **no** form of this command to return to the default setting. Variations of this command include:

egress-queue inherit
egress-queue <*value*>

Syntax Description

inherit	Specifies that traffic egressing the subinterface is mapped to the UNI queue based on the packet's outer tag value.
<*value*>	Specifies the queue to which the traffic is mapped. Valid range is **0** to **7**.

Default Values

By default, egressing traffic inherits the queue information.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that egress traffic from the Layer 3 Ethernet subinterface 1/1.1 is mapped to egress queue **5**:

(config)**#interface ethernet 1/1.1**
(config-eth-1/1.1)**#egress queue 5**

encapsulation 802.1q

Use the **encapsulation 802.1q** command to put the interface into 802.1q virtual local area network (VLAN) mode.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example puts Ethernet interface 0/1 in 802.1q mode and configures a subinterface for VLAN usage:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#encapsulation 802.1q**
(config-eth 0/1)**#interface ethernet 0/1.1**
(config-eth 0/1.1)**#vlan-id 3**

ethernet-cfm down

Use the **ethernet-cfm down** command to enable Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) on the Ethernet interface. Use the **no** form of this command to disable Ethernet OAM CFM on this interface.

Syntax Description

No subcommands.

Default Values

By default, Ethernet OAM CFM is disabled.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

For more information about Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

For more information regarding specific Ethernet OAM CFM configuration commands on the Ethernet interface, refer to the *Ethernet OAM CFM Command Set on page 4405*.

Usage Examples

The following example enables Ethernet OAM CFM on Ethernet interface **0/1**:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ethernet-cfm down**

ethernet-cfm mep

Use the **ethernet-cfm mep** command to create an Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoint (MEP) on the Ethernet interface. Use the **no** form of this command to remove the MEP from the interface. Variations of this command include:

ethernet-cfm mep *<name>* *<name>* *<mep id>* **down**
ethernet-cfm mep none *<name>* *<mep id>* **down**

Syntax Description

<name>	Specifies the MEP's maintenance domain.
<name>	Specifies the MEP's maintenance association.
<mep id>	Specifies the unique numerical ID for this MEP. Range is **1** to **8191**.
none	Optional. Specifies no domain name is used.
down	Specifies the direction of the MEP.

Default Values

By default, no MEPs exist on the interface.

Command History

Release 17.4	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

For more information about Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

For more information about specific MEP configuration commands, refer to the *Ethernet OAM CFM Command Set on page 4405*.

Usage Examples

The following example creates an MEP, with the MEP ID **100**, on Ethernet interface **eth 0/1**. The MEP is associated with maintenance domain **Domain1** and association **association1**:

```
(config)#interface eth 0/1
(config-eth 0/1)#ethernet-cfm mep Domain1 association1 100 down
(config-eth 0/1-mep)
```


ethernet lmi

Use the **ethernet lmi** command to enable Ethernet local management interface (E-LMI) on the Gigabit Ethernet interface. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled. When enabled, the interface is in the provider edge (PE) mode.

Command History

Release R11.5.0	Command was introduced.
Release R11.6.0	Support for monitoring Y.1731 alarms and conditions was added.

Functional Notes

E-LMI is a feature used by AOS to provide user network interface (UNI) and Ethernet virtual connection (EVC) status information to the customer edge (CE) device. Status information is gathered from E-LMI messages exchanged between the PE and CE devices, and is stored in the AOS device.

The **no** form of this command disables E-LMI on the interface and also automatically removes the configured E-LMI bandwidth threshold for the interface, if configured. Refer to the command *ethernet lmi interface <interface> bandwidth-threshold on page 2177*.

Usage Examples

The following example enables the E-LMI feature:

(config)**#interface gigabit-ethernet 0/2**
(config-giga-eth 0/2)**#ethernet lmi**

ethernet lmi interface <*interface*> bandwidth-threshold

Use the **ethernet lmi interface** <*interface*> **bandwidth-threshold** command to monitor the bandwidth of an interface to determine the status of the Ethernet virtual connection (EVC). If the bandwidth of the interface drops below the specified amount, Ethernet local management interface (E-LMI) will indicate that the EVC status is NOT ACTIVE. Use the **no** form of this command to disable the feature. Variations of this command include:

ethernet lmi interface <*interface*> **bandwidth-threshold downspeed** <*value*>
ethernet lmi interface <*interface*> **bandwidth-threshold upspeed** <*value*>
ethernet lmi interface <*interface*> **bandwidth-threshold downspeed** <*value*> **upspeed** <*value*>

Syntax Description

<*interface*>	Specifies the Layer 2 interface to monitor for reduced bandwidth.
downspeed <*value*>	Specifies the bandwidth threshold for traffic moving from the Metro Ethernet network (MEN) to the UNI. If the interface's bandwidth in this direction drops below the specified value, E-LMI will indicate that the EVC is down. Valid range is **0** to **4294967295** kbps. Specifying a value of **0** disables the bandwidth monitoring.
upspeed <*value*>	Specifies the bandwidth threshold for traffic moving from the UNI to the MEN. If the interface's bandwidth in this direction drops below the specified value, E-LMI will indicate that the EVC is down. Valid range is **0** to **4294967295** kbps. Specifying a value of **0** disables the bandwidth monitoring.

Default Values

By default, this feature is disabled.

Command History

Release R11.6.0	Command was introduced.

Functional Notes

E-LMI is a feature used by AOS to provide UNI and EVC status information to the customer edge (CE) device. Status information is gathered from E-LMI messages exchanged between the provider edge (PE) and CE devices, and is stored in the AOS device.

If the actual bandwidth for the specified interface drops below the specified bandwidth, E-LMI indicates that the EVC is active. If the actual bandwidth is greater than or equal to the specified bandwidth, E-LMI indicates that the EVC is active. If both downspeed and upspeed are specified, and if the bandwidth in either direction falls below the specified threshold, E-LMI indicates that the EVC is inactive.

Only one interface can be specified using this command. Entering a different interface over-writes the existing configuration.

Using the **no** version of the command *ethernet lmi on page 2176* also removes the configured E-LMI bandwidth threshold on the interface.

Usage Examples

The following example monitors the downspeed bandwidth for the interface:

(config)**#interface gigabit-ethernet 0/2**
(config-giga-eth 0/2)**#ethernet lmi interface efm-group 1/1 bandwidth-threshold downspeed 400000**

ethernet lmi forwarding

Use the **ethernet lmi forwarding** command to enable transparent forwarding of E-LMI messages from UNI to NNI. Use the **no** form of this command to disable transparent forwarding of E-LMI messages.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled. When enabled, the interface transparently forwards E-LMI messages.

Command History

Release R13.11.0	Command was introduced.

Usage Examples

The following example enables Gigabit Ethernet interface 0/2 to transparently forward E-LMI messages:

(config)**#interface gigabit-ethernet 0/2**
(config-giga-eth 0/2)**#ethernet lmi forwarding**

ethernet oam enable

Use the **ethernet oam enable** command to enable Ethernet Link operations, administration, and management (OAM) on the interface. Use the **no** form of this command to disable Ethernet Link OAM on this interface.

Syntax Description

No subcommands.

Default Values

By default, Ethernet Link OAM is disabled when an interface is created. However, some products have Ethernet OAM enabled in their factory default configuration (for example, the NetVanta 4660).

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables Ethernet Link OAM on Gigabit Ethernet interface **0/1**:

(config)**#interface gigabit-ethernet 0/1**
(config-giga-eth 0/1)**#ethernet oam enable**

ethernet oam mode passive

Use the **ethernet oam mode passive** command to specify the Ethernet Link operations, administration, and management (OAM) mode on the interface. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, Ethernet Link OAM operates in active mode.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

When Ethernet Link OAM is in active mode (default setting), the interface attempts to initiate the OAM discovery process once Ethernet Link OAM is enabled. When Ethernet Link OAM is operating in passive mode, the interface waits for an active peer to initiate OAM discovery, as outlined in IEEE 802.3ah.

Usage Examples

The following example places Ethernet Link OAM in **passive** mode on Gigabit Ethernet interface **0/1**:

(config)**#interface gigabit-ethernet 0/1**
(config-giga-eth 0/1)**#ethernet oam mode passive**

ethernet oam link-monitor

Use the **ethernet oam link monitor** command to allow the interface to receive Ethernet Link operations, administration, and maintenance (OAM) Protocol Data Unit (PDU) Event Notifications on the interface. Use the **no** form of this command to disable OAM PDU Event Notifications on this interface.

Syntax Description

No subcommands.

Default Values

By default, Ethernet Link OAM PDU support is enabled on the interface.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

By default, support for OAM PDUs is advertised during OAM discovery. When OAM is enabled, the interface can receive OAM PDU Event Notifications, OAM PDUs with the Critical Link Event flags set, and Link Event time, length, value (TLV) notifications.

When link events are received by the interface, it keeps a record of the last two unique events on a per-event type basis. This includes critical link events, such as critical events, dying gasps, and link fault notifications, as well as regular link events, such as Errored Symbol Period, Errored Frames, Errored Frame Period, and Errored Frame Seconds Summary TLVs. You can view the recorded local and remote OAM link events using the **show ethernet oam statistics** command as described on *page 634*. You can clear the recorded events using the **clear ethernet oam statistics** command, as described on *page 136*.

Usage Examples

The following example disables support for receiving Ethernet Link OAM PDUs on Gigabit Ethernet interface **0/1**:

(config)**#interface gigabit-ethernet 0/1**
(config-giga-eth 0/1)**#no ethernet oam link-monitor**

ethernet oam mib-retrieval

Use the **ethernet oam mib-retrieval** command to enable Ethernet Link operations, administration, and management (OAM) Protocol Data Unit (PDU) Variable Responses and Variable Requests on the interface. Us the **no** form of this command to disable Variable Response and Request support for this interface.

Syntax Description

No subcommands.

Default Values

By default, Ethernet Link OAM PDU Variable Request and Response support is enabled on the interface.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

By default, support for OAM PDUs is advertised during OAM discovery. When OAM is enabled, the interface can receive OAM PDU Event Notifications, OAM PDUs with the Critical Link Event flags set, and Link Event time, length, value (TLV) notifications.

When link events are received by the interface, it keeps a record of the last two unique events on a per-event type basis. This includes critical link events, such as critical events, dying gasps, and link fault notifications, as well as regular link events, such as Errored Symbol Period, Errored Frames, Errored Frame Period, and Errored Frame Seconds Summary TLVs. You can view the recorded local and remote OAM link events using the **show ethernet oam statistics** as described on *page 634*. You can clear the recorded events using the **clear ethernet oam statistics** command, as described on *page 136*.

Usage Examples

The following example disables support for receiving Ethernet Link OAM PDUs on Gigabit Ethernet interface **0/1**:

(config)**#interface gigabit-ethernet 0/1**
(config-giga-eth 0/1)**#no ethernet oam link-monitor**

flowcontrol receive

Use the **flowcontrol receive** command to enable incoming flow control for the Ethernet interface. If **flowcontrol receive** is enabled, the unit will honor received pause frames. Use the **no** form of this command to disable flow control.

Syntax Description

No subcommands.

Default Values

By default, flow control is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example specifies that Ethernet interface **giga-eth 0/1** honors received pause frames:

(config)**#interface gigabit-ethernet 0/1**
(config-giga-eth 0/1)**#flowcontrol receive**

full-duplex

Use the **full-duplex** command to configure the Ethernet interface for full-duplex operation. This allows the interface to send and receive simultaneously. Use the **no** form of this command to return to the default **half-duplex** operation.

Syntax Description

No subcommands.

Default Values

By default, all Ethernet interfaces are configured for half-duplex operation.

Command History

Release 1.1	Command was introduced.
Release R12.1.0	Command was made unavailable for Ethernet interfaces on virtual AOS (vAOS) instances.

Functional Notes

Full-duplex Ethernet is a variety of Ethernet technology currently being standardized by the IEEE. Because there is no official standard, vendors are free to implement their independent versions of full-duplex operation. Therefore, it is not safe to assume that one vendor's equipment will work with another.

Devices at each end of a full-duplex link have the ability to send and receive data simultaneously over the link. Theoretically, this simultaneous action can provide twice the bandwidth of normal (half-duplex) Ethernet. To deploy full-duplex Ethernet, each end of the link must only connect to a single device (a workstation or a switched hub port). With only two devices on a full-duplex link, there is no need to use the medium access control mechanism (to share the signal channel with multiple stations) and listen for other transmissions or collisions before sending data.

Some Ethernet equipment (though rare) is unable to negotiate duplex if speed is manually determined. To avoid incompatibilities, manually set the duplex if the speed is manually set. Refer to *speed on page 2321* *for more information.*

The 10Base-T, 100Base-TX, and 100Base-FX signaling systems support full-duplex operation (because they have transmit and receive signal paths that can be simultaneously active).

This command is not available for Ethernet interfaces on vAOS instances.

Usage Examples

The following example configures the Ethernet interface for **full-duplex** operation:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#full-duplex**

half-duplex

Use the **half-duplex** command to configure the Ethernet interface for half-duplex operation. This setting allows the Ethernet interface to either send or receive at any given moment, but not simultaneously. Use the **no** form of this command to disable half-duplex operation.

Syntax Description

No subcommands.

Default Values

By default, all Ethernet interfaces are configured for half-duplex operation.

Command History

Release 1.1	Command was introduced.
Release R12.1.0	Command was made unavailable for Ethernet interfaces on virtual AOS (vAOS) instances.

Functional Notes

Half-duplex Ethernet is the traditional form of Ethernet that employs the carrier sense multiple access/collision detect (CSMA/CD) protocol to allow two or more hosts to share a common transmission medium while providing mechanisms to avoid collisions. A host on a half-duplex link must “listen” on the link and only transmit when there is an idle period. Packets transmitted on the link are broadcast (so it will be “heard” by all hosts on the network). In the event of a collision (two hosts transmitting at once), a message is sent to inform all hosts of the collision and a backoff algorithm is implemented. The backoff algorithm requires the station to remain silent for a random period of time before attempting another transmission. This sequence is repeated until a successful data transmission occurs.

Some Ethernet equipment (though rare) is unable to negotiate duplex if speed is manually determined. To avoid incompatibilities, manually set the duplex if the speed is manually set. Refer to *speed on page 2321* *for more information.*

This command is not available for Ethernet interfaces on vAOS instances.

Usage Examples

The following example configures the Ethernet interface for **half-duplex** operation:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#half-duplex**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for IPv4 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Applies the named IPv4 ACL to the interface.
in	Enables access control on IPv4 packets received on the specified interface.
out	Enables access control on IPv4 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example configures the router to only allow IPv4 Telnet traffic (as defined in the user-configured **TelnetOnly** ACL) into the Ethernet interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface ethernet 0/1**
(config-eth 0/1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the Ethernet interface 0/1:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ip access-policy PRIVATE**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii *<string>* **| hex** *<value>***] [client-id [***<interface>* **|** *<identifier>***]] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp client-id [*<interface>* **|** *<identifier>***] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp hostname *"<string>"* **[no-default-route | no-domain-name | no-nameservers] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track *<name>***] [***<administrative distance>***]**
ip address dhcp track *<name>* **[***<administrative distance>***]**

Syntax Description

<administrative distance>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii *<string>*	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex *<value>*	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<interface>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<identifier>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the *<identifier>* option.
hostname *<"string">*	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

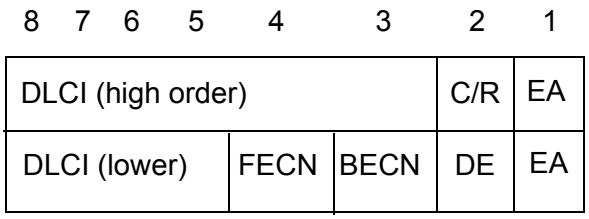
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *“<string>”* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the Ethernet interface 0/1:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip address dhcp**

The following example enables DHCP operation on the Ethernet interface 0/1 utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip address dhcp hostname “adtran” no-default-route no-domain-name no-nameservers 5**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface (only one primary address is allowed). Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 /30**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip address 192.22.72.101 /30 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

> NOTE *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.*

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

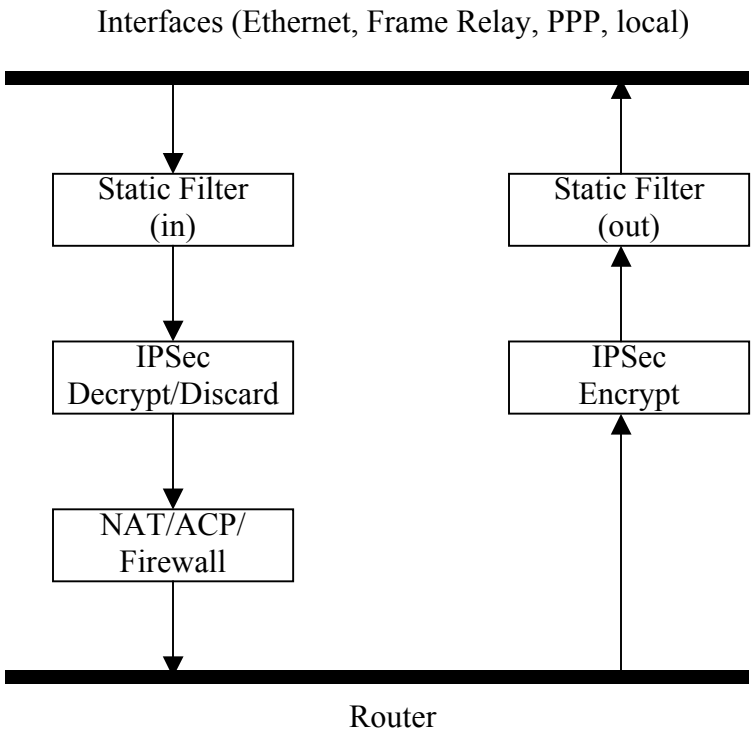
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Level Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the Ethernet interface:

(config)**#ethernet 0/1**
(config-eth 0/1)**#ip crypto map MyMap**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).

Usage Examples

The following example releases the IPv4 address assigned (by DHCP) on the Ethernet interface 0/1:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip dhcp release**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Optional. Specifies an IP access control list (ACL) to filter traffic.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **ethernet 0/1**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 4 (IPv4) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries to be cleared from this IPv4 interface.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.4.0	Maximum number of stored entries was expanded to **500000** and RapidRoute is now enabled by default.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv4 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#no ip ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example enables traffic monitoring on an **Ethernet** interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

*The **ip helper-address** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.

2. Any UDP port specified using the **ip forward-protocol** command.

3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).

4. The destination IP address is broadcast defined by all ones (**255.255.255.255**) or a subnet broadcast (for example, **192.33.4.251** for the **192.33.4.248 /30** subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

The defaults for this command are:

last-member-query-interval	**1000** milliseconds
querier-timeout	2x the **query-interval** value
query-interval	**60** seconds
query-max-response-time	**10** seconds
version	Version **1**

There are no default values for **immediate-leave** and **static-group**.

Command History

Release 7.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface, and to place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 2210* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip mcast-stub downstream**

ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*ip address*> command to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 2207*, and *ip mcast-stub upstream on page 2210* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 2207* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces (all types)	1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

OSPFv2 will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the Ethernet interface 0/1:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example specifies an OSPFv2 priority of **120** on the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip ospf 1 priority 120**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<process id>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip ospf 1 network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the Ethernet 0/1 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the Ethernet 0/1 interface every **3600** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example sets the neighbor timeout to **300** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example sets the propagation delay to **300** milliseconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route-map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only RIP version 1 packets received on the interface.
2	Accepts only RIP version 2 packets received on the interface.

Default Values

By default, all interfaces implement RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only accepts one version (either **1** or **2**) on a given interface.

Usage Examples

The following example configures the Ethernet interface to accept only RIP version **2** packets:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only transmits one version (either **1** or **2**) on a given interface.

Usage Examples

The following example configures the Ethernet interface to transmit only RIP version **2** packets:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable Internet Protocol version 4 (IPv4) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Fast switching allows an IPv4 interface to provide optimum performance when processing IPv4 traffic.

Usage Examples

The following example enables IPv4 fast switching on the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 11.1	Command was expanded to include the demand interfaces.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered ppp 1** while in the Ethernet Interface Configuration mode configures the Ethernet interface to use the IP address assigned to the Point-to-Point Protocol (PPP) interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the Ethernet interface 0/1 to use the IP address assigned to the PPP interface (**ppp 1**):

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip unnumbered ppp 1**

ip urlfilter *<name>*

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter *<name>* **in**
ip urlfilter *<name>* **out**

Syntax Description

<name>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** *<filtername>* **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the Ethernet interface and matches the URL filter named **MyFilter**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on an interface. Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the interface.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the interface to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the interface.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an interface when other unicast IPv6 addresses are not needed on the interface. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the interface.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6**

ipv6 access-group *<ipv6 acl name>*

Use the **ipv6 access-group** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to be used for IPv6 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ipv6 access-group *<ipv6 acl name>* **in**
ipv6 access-group *<ipv6 acl name>* **out**

Syntax Description

<ipv6 acl name>	Applies the named IPv6 ACL to the interface.
in	Enables access control on IPv6 packets received on the specified interface.
out	Enables access control on IPv6 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 18.1	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Only one IPv6 ACL can be applied in each traffic direction.

Unlike in IPv4, IPv6 traffic filters include an implicit **permit** for neighbor solicitation and advertisement packets in an ACL before the traditional implicit **deny** at the end of the ACL. This prevents blocking of address resolution and unreachability detection, although this can be overridden by entering explicit **deny** commands in the IPv6 ACL.

Usage Examples

The following example applies the IPv6 ACL **Privatev6** to incoming IPv6 traffic on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 access-group Privatev6 in**

ipv6 access-policy *<ipv6 acp>*

Use the **ipv6 access-policy** command to assign a specified Internet Protocol version 6 (IPv6) access control policy (ACP) to an interface. IPv6 ACPs are applied to IPv6 traffic entering an interface. Use the **no** form of this command to remove an ACP association.

Syntax Description

<ipv6 acp>	Identifies the configured IPv6 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv6 ACPs associated with an interface.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example applies the IPv6 ACP **PRIVATEv6** to the interface:

Enable the AOS security features:
(config)**#ipv6 firewall**

Associate the ACP with the Ethernet interface 0/1:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ipv6 access-policy PRIVATEv6**

ipv6 address autoconfig

Use the **ipv6 address autoconfig** command to enable Internet Protocol version 6 (IPv6) processing on the interface, create a local-link IPv6 address for the interface, and allow the interface to automatically configure itself based on advertisements from other routers on the link. Use the **no** form of this command to remove all autoconfigured addresses, prefixes, and any resulting routes from the interface and also causes the interface to cease processing received router advertisements (RAs).Variations of this command include:

ipv6 address autoconfig
ipv6 address autoconfig default
ipv6 address autoconfig default metric <*value*>

Syntax Description

default	Optional. Specifies that the interface maintain a list of advertising routers that are willing to be IPv6 default routers.
metric <*value*>	Optional. Specifies the administrative distance for a default router maintained in the default router list. Range is **1** to **255**. Routes with lower administrative distance are favored.

Default Values

By default, no IPv6 addresses are configured for the interface and IPv6 processing is not enabled. When an IPv6 address is configured automatically, the administrative distance for default routers is **2** by default.

Command History

Release 18.1	Command was introduced.

Functional Notes

When autoconfiguration is enabled, the interface listens for RA messages that tell the interface how it should be configured. The interface then creates addresses for advertised 64-bit prefixes with the A flag in the IPv6 address set using stateless address autoconfiguration (SLAAC). The addresses use the EUI-64 interface ID in the lower 64 bits of the address. A route type of *Connected* is added to the route table if the L flag on the prefix advertisement (on-link flag) is also set.

Usage Examples

The following example enables IPv6 processing on the interface, creates a link-local IPv6 address for the interface, and allows the interface to automatically configure itself for IPv6:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 address autoconfig**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 2237*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 2237*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the interface and enables IPv6 processing on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address <*ipv6 link-local address*> link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<*ipv6 link-local address*>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the interface.

Default Values

By default, no IPv6 address is configured for the interface and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

A single link-local address can be manually configured on an interface. The lower 64 bits of the specified address become the Interface ID for the interface, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the interface and can be derived from the interface's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the interface.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example manually creates a link-local IPv6 address on the interface and enables IPv6 processing:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 crypto map *<name>*

Use the **ipv6 crypto map** command to associate Internet Protocol version 6 (IPv6) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

Syntax Description

<name>	Specifies the IPv6 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Only one IPv6 crypto map can be specified per interface, and the crypto map is applied within the virtual routing and forwarding (VRF) instance to which the interface belongs. To apply the IPv6 crypto map, the interface must have IPv6 enabled. In addition, the interface must have an IPv6 address of appropriate scope to allow connectivity to peer's addresses as specified in the crypto map's entries.

Usage Examples

The following example applies all IPv6 crypto maps with the name **MyMap** to the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6**
(config-eth 0/1)**#ipv6 crypto map MyMap**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname *<partial fqdn>*
ipv6 address dhcp hostname fqdn *<fqdn>*
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 2231*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 address 2001:DB8:1::1/64**
(config-eth 0/1)**#ipv6 address dhcp fqdn client@company.com**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)#ipv6 dhcp client pd PREFIX1

ipv6 dhcp relay destination *<ipv6 address>*

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address or Ethernet virtual circuit (EVC) for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination *<ipv6 address>*
ipv6 dhcp relay destination *<ipv6 address>* *<interface>*
ipv6 dhcp relay destination *<ipv6 address>* **mef-ethernet** *<slot/port>*
ipv6 dhcp relay destination *<ipv6 address>* **system-control-evc**
ipv6 dhcp relay destination *<ipv6 address>* **system-management-evc**

Syntax Description

<ipv6 address>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** *<ipv6 address>* **?** to display a list of valid interfaces.
mef-ethernet *<slot/port>*	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the DHCPv6 messages are sent to the IPv6 address on the system control EVC.
system-management-evc	Optional. Specifies the DHCPv6 messages are sent to the IPv6 address on the system management EVC.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the **system-control-evc** and **system-management-evc** for the Layer 3 Ethernet and Gigabit Ethernet subinterfaces.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.
Release R13.7.0	Command was expanded to include the VLAN interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command *ipv6 on page 2231*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination IPv6 address as **2001:DB8:2::1**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6**
(config-eth 0/1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped multicast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the interface and specify that the interface is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the interface, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the interface. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this interface. All DHCPV^ requests received on this interface are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Enabling the interface as a DHCPv6 server using this command places the interface into DHCPv6 server mode. DHCPv6 modes (server or relay) are mutually exclusive at the interface. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the interface as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 address 2001:DB8:1::1/64**
(config-eth 0/1)**#ipv6 dhcp server POOL1**

ipv6 ffe

Use the **ipv6 ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 6 (IPv6) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 ffe
ipv6 ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries to be cleared from this IPv6 interface.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled on IPv6-enabled interfaces (using the command *ipv6 on page 2231*). The default number of **max-entries** is **4096**.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv6 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#no ipv6 ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the interface in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the interface.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the interface in host mode:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 mode host unicast**

ipv6 mtu *<size>*

Use the **ipv6 mtu** command to specify the maximum transmission unit (MTU) for Internet Protocol version 6 (IPv6) packets on the interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Specifies the MTU value. Valid range is **1280** to **1500** bytes.

Default Values

By default, the MTU of the interface is set to **1280** bytes.

Command History

Release 18.1	Command was introduced.

Functional Notes

In IPv6, the minimum MTU is 1280 octets. Any link that has an MTU less than 1280 octets must use link fragmentation and reassembly that is transparent to IPv6 (for example, the Fragmentation Header). Sources in the IPv6 network are expected to perform path maximum transmission unit (PMTU) discovery to send packets larger than 1280 octets. PMTU works in the following manner: First, the sending node assumes the link MTU of the interface from which the traffic is being forwarded and then sends the IPv6 packet at the link MTU size. If a router on the path is unable to forward the packet, it sends an ICMP *Packet Too Big* message back to the sending node containing the link MTU of the link on which the packet forwarding failed. The sending node then rests the PMTU to the value of the MTU field in the Internet Control Message Protocol version 6 (ICMPv6) *Packet Too Big* message, and the packet is resent.

The MTU for IPv6 packets can be set on a per-interface basis. There are two methods for setting MTUs for interfaces if required: one for Layer 3 interfaces, and one for the underlying Layer 1 and Layer 2 interfaces. For all interface types, use the **ipv6 mtu** *<size>* command to specify the IPv6 MTU in bytes from the interface's configuration mode. The minimum MTU setting for IPv6 is **1280** bytes, and the maximum is **1500** bytes. The IPv6 MTU value is independent of the IPv4 MTU setting (set with the command *ip mtu <size> on page 2211*).

When the interface is forwarding the IPv6 packet as a router, if the packet size exceeds the IPv6 MTU of the egress interface, the packet is dropped and ICMPv6 *Packet Too Big* message is sent to the source. When originating an IPv6 packet from the local IPv6 stack, and the packet is larger than the IPv6 MTU of the egress interface, the packet is fragmented and sent.

Usage Examples

The following example specifies the IPv6 MTU value for the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 mtu 1350**

ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** command to specify that the Advertisement Interval Option is sent in Internet Protocol version 6 (IPv6) router advertisement (RA) messages from the router. This command is effectual only when the interface is in router mode. Use the **no** form of this command to return to the default interval.

Syntax Description

No subcommands.

Default Values

By default, Advertisement Interval Options are not sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

Sending the Advertisement Interval Option should be enabled when the router is functioning in a mobile IP environment to aid movement detection by mobile nodes. This option contains the current value of the maximum router advertisement interval configured using the command *ipv6 nd ra interval on page 2259*.

Usage Examples

The following example specifies that the interface include Advertisement Interval Options in RA messages sent from the router:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd advertisement-interval**

ipv6 nd cache max-incomplete <*number*>

Use the **ipv6 nd cache max-incomplete** command to specify the maximum number of incomplete entries the Neighbor Discovery (ND) cache retains. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of incomplete ND entries to retain in the cache. Valid range is **1** to **321**.

Default Values

By default, the incomplete ND entries can take at maximum one-third of the possible ND cache entries (varies by product).

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example specifies that the interface stores **150** incomplete entries in the ND cache:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd cache max-incomplete 150**

ipv6 nd dad attempts *<number>*

Use the **ipv6 nd dad attempts** command to specify the number of neighbor solicitation (NS) messages sent by the interface when performing Internet Protocol version 6 (IPv6) duplicate address detection (DAD). This command is effectual when the interface is in either host or router mode. Use the **no** form of this command to return to the default value.

Syntax Description

<number>	Specifies the number of NS messages that will be sent. Range is **0** to **10** messages. A value of **0** disables DAD on the interface.

Default Values

By default, the interface sends **1** NS message.

Command History

Release 18.1	Command was introduced.

Functional Notes

DAD is used by devices to determine if IPv6 addresses are unique before they are applied to interfaces. DAD is used in NS messages to detect duplicate unicast addresses. The Target Address fields in the NS messages are set to the IPv6 address for which duplication is being detected. Destination IPv6 addresses for DAD in NS messages are the solicited-node multicast version of the address being tested. Source IPv6 addresses for DAD are set to the IPv6 unspecified address (::). Once the IPv6 address is determined by DAD to be unique, it can be applied to the IPv6 interface on the node.

DAD in AOS is performed when an interface transitions state from DOWN to UP or when manually configuring an address. When performing DAD because of an interface transition, DAD will happen immediately after the interface transition and again 40 seconds later to cooperate with the port being connected to an Ethernet switch.

Usage Examples

The following example specifies that **3** NS messages are sent by the interface when performing DAD:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd dad attempts 3**

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command to specify the M flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. The M flag instructs hosts receiving the RA that they can use stateful Dynamic Host Configuration Protocol version 6 (DHCPv6) to configure addresses and other information. Use the **no** form of this command to disable the setting of the M flag.

Syntax Description

No subcommands.

Default Values

By default, the M flag is not set in RAs.

Command History

Release 18.1	Command was introduced.

Functional Notes

If you specify that the M flag is set in RA messages, you do not need to set the 0 flag (it becomes redundant).

Usage Examples

The following example sets the M flag for RA messages sent by the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd managed-config-flag**

ipv6 nd ns-interval *<value>*

Use the **ipv6 nd ns-interval** command to specify the interval between transmission of certain Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages and to control what ND value is advertised in router advertisement (RA) messages. This command is effectual whether the interface is in host or router mode. Use the **no** form of this command to return the interval to the default value.

Syntax Description

<value>	Specifies the time (in milliseconds) between neighbor message transmissions. Valid range is **1000** to **3600000** ms.

Default Values

By default, the interval is set to **1000** ms for internal use by the router and **0** (unspecified) is sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command controls the spacing of neighbor solicitation (NS) messages for functions such as address resolution, reachability detection, and duplicate address detection (DAD). For DAD it also serves as the amount of time after the last transmission before the detection phase of autoconfiguration terminates. In addition, the command controls the interval between unsolicited neighbor advertisement (NA) messages.

Usage Examples

The following example changes the interval between RA messages sent from the interface to **2000** ms:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd ns-interval 2000**

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command to specify the O flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. When the O flag is set, hosts receiving the RA messages are instructed that they may use stateless Dynamic Host Configuration Protocol version 6 (DHCPv6) to receive information that is not IPv6 addressing information, and to use some other method (whether through manual configuration, stateless address autoconfiguration (SLAAC), etc.) for addressing information. Use the **no** form of this command to disable the O flag setting.

Syntax Description

No subcommands.

Default Values

By default, the O flag is not set in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

If the M flag is set for RA messages, you do not need to set the O flag.

Usage Examples

The following example sets the O flag in RA messages from the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd other-config-flag**

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the interface. Use the **no** form of this command to remove the specified prefix configuration from the interface. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the interface is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the interface. Prefixes for IPv6 addresses configured on a router interface are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the interface.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ipv6 nd purge-timer <*value*>

Use the **ipv6 nd purge-timer** command to specify the maximum amount of time an unused Internet Protocol version 6 (IPv6) neighbor entry remains in the neighbor cache. This command applies to interfaces in either host or router mode. Use the **no** form of this command to return the purging interval to the default value.

Syntax Description

<*value*>	Specifies the neighbor cache entry storage time in minutes. Valid range is **10** to **1440** minutes.

Default Values

By default, idle (STALE) neighbor cache entries are cleared after **1440** minutes (24 hours).

Command History

Release 18.1	Command was introduced.

Functional Notes

This command applies to interfaces in either router or host mode. A neighbor entry is typically purged when neighbor unreachability detection (NUD) is invoked and the neighbor is determined to no longer be reachable. However, NUD is not performed on idle (STALE) neighbor entries, so this command provides a method for purging unused entries after a specified amount of time.

Usage Examples

The following example specifies that idle neighbor entries in the neighbor cache are removed after **800** minutes:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd purge-timer 800**

ipv6 nd ra interval

Use the **ipv6 nd ra interval** command to specify the interval between transmission of Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 nd ra interval *<max time>*
ipv6 nd ra interval *<max time> <min time>*
ipv6 nd ra interval msec *<max time>*
ipv6 nd ra interval msec *<max time> <min time>*

Syntax Description

<max time>	Specifies the maximum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **4** to **1800** seconds and **70** to **1800000** ms.
<min time>	Optional. Specifies the minimum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **3** seconds to 75 percent of the configured maximum time value in seconds, or **30** ms to 75 percent of the configured maximum time value in ms.
msec	Optional. Specifies that the time values are in milliseconds.

Default Values

By default, the interval is set in seconds and has a maximum interval time of **200** seconds and a minimum interval time of 75 percent of the maximum seconds value, but not less than **3** seconds.

Command History

Release 18.1	Command was introduced.

Functional Notes

If this router is used as a default router, the interval between RA messages should not be set to a larger value than the RA lifetime set by the command *ipv6 nd ra lifetime <value> on page 2260*, which has a default value of **1800** seconds.

Usage Examples

The following example specifies that the maximum interval in seconds between RA message transmissions is **300**:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ipv6 nd ra interval 300**

ipv6 nd ra lifetime <*value*>

Use the **ipv6 nd ra lifetime** command to specify the router lifetime advertised in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is effectual when the interface is in router mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

ipv6 nd ra lifetime <*value*>
ipv6 nd ra lifetime default-route

Syntax Description

<*value*>	Specifies the router lifetime in seconds. Range is **0** to **9000** seconds. A value of **0** indicates this is not a default router. A value other than 0 indicates to other nodes that this router can be used as a default router.
default-route	Specifies that the RA lifetime is **0** if no default route exists on any IPv6 interface.

Default Values

By default, the router lifetime is set to **1800** seconds.

Command History

Release 18.1	Command was introduced.
Release R11.5.0	Command was expanded to include the **default-route** parameter.

Functional Notes

A value other than **0** for a router lifetime should be larger than the router advertisement interval specified in the command *ipv6 nd ra interval on page 2259*.

Usage Examples

In the following example, the router lifetime advertised in RA messages is **3000** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd ra lifetime 3000**

ipv6 nd ra reachable-time <*value*>

Use the **ipv6 nd ra reachable-time** command to specify the value advertised for reachable time in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command also specifies the internal base reachable time used by the router. This command is effectual for interfaces in either host or router mode. Use the **no** form of this command to return the reachability value to the default setting.

Syntax Description

<*value*>	Specifies the reachability time in milliseconds. Range is **0** to **3600000** ms. A value of **0** indicates the reachable time is unspecified.

Default Values

By default, the router advertises a reachability time of **0** ms and uses an internal value of **30000** ms.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command is effectual for interfaces in either router or host mode. For hosts, this value sets the internal reachable time used by the host if no RAs are received specifying a different value. For routers, the value indicates the amount of time a device is considered reachable after having received a reachability confirmation in neighbor unreachabililty detection (NUD).

Usage Examples

The following example specifies that a reachability time of **50000** ms is advertised in RA messages:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd ra reachable-time 50000**

ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command to specify whether Internet Protocol version 6 (IPv6) router advertisement (RA) messages will be suppressed. This command only applies to interfaces in router mode. Use the **no** form of this command to begin sending RA messages.

Syntax Description

No subcommands.

Default Values

By default, RA messages are not suppressed. When IPv6 routing is not enabled on the router, or when implemented in a host-only mode, the default setting is to suppress advertisements on all interface types.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example suppresses RA messages on the interface:

(config)**#interface eth 0/1**
(config-eth 0/1)**#ipv6 nd ra suppress**

ipv6 nd router-preference

Use the **ipv6 nd router-preference** command to specify the default router preference value set in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. Setting this preference helps the receivers of RA messages to determine the preference of one router over another as a default router in environments with multiple routers. Use the **no** form of this command to return the preference to the default setting. Variations of this command include:

ipv6 nd router-preference high
ipv6 nd router-preference low
ipv6 nd router-preference medium

Syntax Description

high	Specifies the preference value is high.
low	Specifies the preference value is low.
medium	Specifies the preference value is medium.

Default Values

By default, the router preference is set to medium.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that the advertised default router preference is high:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 nd router-preference high**

ipv6 route-cache

Use the **ipv6 route-cache** command to enable Internet Protocol version 6 (IPv6) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 18.2	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Fast switching allows an IPv6 interface to provide optimum performance when processing IPv6 traffic.

Usage Examples

The following example enables IPv6 fast switching on the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 route-cache**

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to prevent LLDP packets from being received on the interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 8.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example configures Ethernet interface 0/1 to receive LLDP packets:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to prevent certain information from being transmitted by the interface. Variations of this command include:

lldp send 802.3-info mac-phy-config
lldp send management-address
lldp send med-info network-policy
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

802.3-info mac-phy-config	Enables transmission of the capability and settings of the duplex and speed on this interface.
management-address	Enables transmission of management address information on this interface.
med-info network-policy	Enables transmission of LLDP-Media Endpoint Discovery (LLDP-MED) network policy information on the interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets. This is the default setting.

Default Values

By default, all interfaces that support LLDP except routed Ethernet are configured to transmit and receive LLDP packets. LLDP is disabled by default on routed Ethernet interfaces.

The 802.3 MAC/PHY status configuration and LLDP-MED network policy time length values (TLVs) are only supported on switchport interfaces and NetVanta 1524ST Gigabit Ethernet interfaces.

Command History

Release 8.1	Command was introduced.
Release 17.2	Command was expanded to include the 802.3 and LLDP-MED information.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures Ethernet interface 0/1 to transmit LLDP packets containing all enabled information types:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#lldp send**

The following example configures Ethernet interface 0/1 to transmit and receive LLDP packets containing all enabled information types:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#lldp send-and-receive**

mac access-group *<mac acl name>*

Use the **mac access-group** command to associate a media access control (MAC) access control list (ACL) with the interface. When applied, these ACLs provide source MAC address filtering on the interface. Use the **no** form of this command to remove the ACL from the interface.

Syntax Description

<mac acl name>	Specifies the name of the previously created MAC ACL to associate with the interface.

Default Values

By default, no MAC ACLs are configured.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example associates the MAC ACL **MACACL1** with the Gigabit Ethernet interface:

(config)**#interface gigabit-ethernet 0/2**
(config-giga-eth 0/2)**#mac access-group MACACL1**

mac-address *<mac address>*

Use the **mac-address** command to specify the medium access control (MAC) address of the unit. Only the last three values of the MAC address can be modified. The first three values contain the Adtran reserved number (00:0A:C8) by default. Use the **no** form of this command to return to the default MAC address programmed by Adtran.

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

A unique default MAC address is programmed in each unit shipped by Adtran.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Gigabit Ethernet interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example configures a MAC address of **00:0A:C8:5F:00:D2**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#mac-address 00:0A:C8:5F:00:D2**

mac aging-time *<value>*

Use the **mac aging-time** command to specify the time that a media access control (MAC) address is considered valid on the interface. Use the **no** form of this command to return the aging time to the default value.

Syntax Description

<value>	Specifies the time, in seconds, that a MAC address is considered valid. Valid range is **0** to **3600** seconds. A value of **0** forces learn and lock behavior.

Default Values

By default, a MAC address is considered valid for **300** seconds.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example sets the MAC address aging time to **1000** seconds:

(config)**#interface gigabit-ethernet 0/2**
(config-giga-eth 0/2)**#mac aging-time 1000**

mac limit *<value>*

Use the **mac limit** command to specify the maximum number of media access control (MAC) addresses to be learned on the interface. This limit pulls from a global pool of 1024 learnable MAC addresses. In addition, when MAC limits are enabled on an interface with a MAC access control list (ACL) applied, addresses are learned that match the ACL up to the specified limit. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the number of MAC addresses to be learned on the interface. Valid range is **1** to **1024**.

Default Values

By default, no MAC address limits are enforced on the interface.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example specifies a limit of **500** MAC addresses can be learned on the interface:

(config)**#interface gigabit-ethernet 0/2**
(config-giga-eth 0/2)**#mac limit 500**

max-reserved-bandwidth *<value>*

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<value>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.

Usage Examples

The following example specifies **85** percent of the bandwidth on the Ethernet interface 0/1 be available for use in user-defined queues:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#max-reserved-bandwidth 85**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip primary vrrp <*number*>
media-gateway ip primary vrrpv3 <*number*>
media-gateway ip secondary <*ipv4 address*>
media-gateway ip secondary vrrp <*number*>
media-gateway ip secondary vrrp <*number*> <*ipv4 address*>
media-gateway ip secondary vrrpv3 <*number*>
media-gateway ip secondary vrrpv3 <*number*> <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrrp <*number*>	Specifies that the IPv4 address of the Virtual Router Redundancy Protocol version 2 (VRRP) router group's virtual router ID (VRID) is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
vrrpv3 <*number*>	Specifies that the IPv4 address of the VRRP version 3 (VRRPv3) VRID is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
<*ipv4 address*>	Optional. Specifies a secondary IPv4 address of the VRRP or VRRPv3 VRID is used as the media gateway address on the interface. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A4.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.
Release R12.2.0	Command was expanded to include the **vrrp** and **vrrpv3** parameters.

Functional Notes

To use VRRP or VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRP or VRRPv3.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#media-gateway ip primary**

media-gateway ipv6

Use the **media-gateway ipv6** command to associate an Internet Protocol version 6 (IPv6) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv6 address associated with it. However, some interfaces allow dynamic configuration of IPv6 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ipv6
media-gateway ipv6 <*ipv6 address*>
media-gateway ipv6 loopback <*interface id*>
media-gateway ipv6 vrrpv3 <*number*>
media-gateway ipv6 vrrpv3 <*number*> <*ipv6 address*>

Syntax Description

<*ipv6 address*>	Specifies an IPv6 address to use for the media gateway. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
loopback <*interface id*>	Specifies an IPv6 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv6 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
vrrpv3 <*number*>	Specifies that all the secondary IPv6 addresses of the Virtual Routing Redundancy Protocol version 3 (VRRPv3) virtual router ID (VRID) are used as media gateway addresses on the interface. Valid VRID range is **1** to **255**.
<*ipv6 address*>	Optional. Specifies a single IPv6 address of the VRRPv3 VRID is used as the media gateway address on the interface. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

Default Values

By default, **media-gateway ipv6** is disabled.

Command History

Release R10.8.0	Command was introduced.
Release R12.2.0	Command was expanded to include the **vrrpv3** parameters.

Functional Notes

To use VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRPv3.

Usage Examples

The following example configures the unit to use the IPv6 address for RTP traffic:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#media-gateway ipv6**

men-c-tag <*value*>

Use the **men-c-tag** command to specify the C-tag used to identify traffic on the Layer 3 subinterface within an Ethernet virtual connection (EVC). Use the **no** form of this command to remove the C-tag value.

Syntax Description

<*value*>	Specifies the value for the C-tag. Valid range is **1** to **4094**.

Default Values

By default, the C-tag is not specified.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies a C-tag value of **100** for the traffic associated with the Layer 3 Gigabit Ethernet subinterface 1/1.1:

(config)**#interface gigabit-ethernet 1/1.1**
(config-giga-eth-1/1.1)**#men-c-tag 100**

men-c-tag-pri

Use the **men-c-tag-pri** command to specify the default priority used by the C-tag. The C-tag is used to identify traffic on the Layer 3 subinterface within an Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default value. Variations of this command include:

men-c-tag-pri inherit
men-c-tag-pri <*value*>

Syntax Description

inherit	Specifies that the C-tag inherits the priority of the S-tag.
<*value*>	Specifies the C-tag default priority. Valid range is **0** to **7**.

Default Values

By default, the C-tag priority is set to **inherit**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies the C-tag priority as **6** on the Layer 3 Gigabit Ethernet subinterface 1/1.1:

(config)**#interface gigabit-ethernet 1/1.1**
(config-giga-eth-1/1.1)**#men-c-tag-pri 6**

men-pri

Use the **men-pri** command to specify the default value of the S-tag used in Ethernet virtual connection (EVC) communication. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-pri inherit
men-pri <*value*>

Syntax Description

inherit	Specifies that the S-tag priority value is inherited from the customer equipment (CE) virtual local area network (VLAN).
<*value*>	Specifies a priority value for the S-tag. Valid range is **0** to **7**.

Default Values

By default, the S-tag is set to **inherit**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that the S-tag has a priority of **5** on the Layer 3 Gigabit Ethernet subinterface 1/1.1:

(config)**#interface gigabit-ethernet 1/1.1**
(config-giga-eth-1/1.1)**#men-pri 5**

men-queue

Use the **men-queue** command to specify the output queue used by the Ethernet virtual connection (EVC) for traffic egressing this Layer 3 subinterface. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-queue inherit
men-queue <*value*>

Syntax Description

inherit	Specifies that traffic egressing the subinterface is mapped to the Metro Ethernet network (MEN) queue based on the packet's outer tag value.
<*value*>	Specifies the queue to which the traffic is mapped. Valid range is **0** to **7**.

Default Values

By default, egressing traffic inherits the queue information.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that egress traffic from the Layer 3 Gigabit Ethernet subinterface 1/1.1 inherits the queue mapping information:

(config)**#interface gigabit-ethernet 1/1.1**
(config-giga-eth-1/1.1)**#men-queue inherit**

mtu <*size*> include-l2-header

Use the **mtu** <*size*> **include-l2-header** command to specify the maximum transmission unit (MTU) for the Layer 2 user network interface (UNI). Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Specifies the MTU size in bytes. Valid range is **60** to **9242** bytes.
include-l2-header	Specifies that the Layer 2 header, any tags, and the Layer 2 payload are included in the MTU size.

Default Values

By default, the MTU on Layer 2 interfaces is set to **9242** bytes.

Command History

Release R11.7.0	Command was introduced.

Functional Notes

This command specifies the MTU for Layer 2 interfaces only. This MTU size includes the Layer 2 header, any associated tags, and the Layer 2 payload, but not the frame check sequence (FCS). If the Layer 2 MTU is configured to be below the MTU for the Layer 3 interface, a misconfiguration occurs and as a result, traffic can be lost. To avoid a misconfiguration, a warning is displayed whenever the Layer 2 MTU is configured below 1526 bytes.

Usage Examples

The following example configures the MTU for the Layer 2 Gigabit Ethernet interface:

(config)**#interface gigabit-ethernet 0/1**
(config-giga-eth 0/1)**#mtu 4400 include-l2-header**

no shutdown track *<name>*

Use the **no shutdown track** command to restore the gigabit switchport interface when the specified track passes. For more information about tracks, refer to *track <name> on page 1886* and the *Network Monitor Track Command Set on page 4098*.

Syntax Description

<name>	Specifies the name of the track to associate with the activation of the interface.

Default Values

By default, this command is not configured.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example enables the interface based on the specified track:

(config)**#interface gigabit-switchport 0/1**
(config-giga-swx 0/1)**#no shutdown track work-hours**

ospfv3 <*process id*> **area** <*area id*>

Use the **ospfv3 area** command to add an interface to an Open Shortest Path First version 3 (OSPFv3) process, and to configure the OSPFv3 process on the interface. This command places the interface in the specified area for the specified Internet Protocol version 6 (IPv6) OSPFv3 address family, and optionally defines the instance ID that is used to represent this OSPFv3 process in messages on the interface's link. Use the **no** form of this command to remove the OSPFv3 process from the interface. Variations of this command include:

ospfv3 <*process id*> **area** <*area id*> **ipv6**
ospfv3 <*process id*> **area** <*area id*> **ipv6 instance** <*instance id*>

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join, for the specified address family. The process ID is locally significant to the device, and must be unique among all OSPFv3 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the given OSPFv3 process. Valid range is **0** to **4294967295**.
ipv6	Identifies the OSPFv3 address family as IPv6.
instance <*instance id*>	Optional. Specifies the value to use in the instance ID field of messages sent or received by this OSPFv3 process on the interface's link. Valid range is **0** to **31**.

Default Values

By default, an OSPFv3 process is not configured on an interface. By default, process IDs, area IDs, and instance IDs are not defined.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

When using this command to enable an OSPFv3 process on an interface, keep the following rules in mind:

- The interface must have the address family enabled on the interface. If the address family is not enabled on the interface, the command is rejected and an error is displayed.
- Only interfaces on the default virtual routing and forwarding (VRF) instance support this command. Interfaces on a nondefault VRF will display an error when you attempt to configure OSPFv3 settings.
- The interface and the specified OSPFv3 process (if defined in the global configuration) must be in the same VRF or the command will fail.
- The address family must match that specified for the OSPFv3 process if the process has been defined in the global configuration or the command will fail.
- If the OSPFv3 process identified by the process ID does not exist in the global configuration, it is automatically created, along with the specified address family, and it is assigned to the VRF of which the interface is a member.

- If the specified OSPFv3 process is already at its maximum limit of processes or address families, the command fails.
- If the specified OSPFv3 process already exists in the global configuration, but its configuration does not include an address family, the specified address family is added to the OSPFv3 router configuration.
- A given OSPFv3 process can only have one address family.
- Multiple OSPFv3 instances per address family, per VRF, can be created and can be assigned to a given interface.
- If the interface's VRF changes, all OSPFv3 assignments are removed.
- To change an OSPFv3 process's VRF, the process must first be removed and then recreated. Removing the process removes all OSPFv3 assignments for that process form all interfaces.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To add an interface to the OSPFv3 process **5**, in area **10**, with an instance ID of **10**, enter the command as follows:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 5 area 10 ipv6 instance 10**

ospfv3 authentication

Use the **ospfv3 authentication** command to authenticate an interface that is performing Internet Protocol version 6 (IPv6) Open Shortest Path First version 3 (OSPFv3) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ospfv3 authentication ipsec spi <*spi*> **md5** <*key*>
ospfv3 authentication ipsec spi <*spi*> **sha1** <*key*>
ospfv3 authentication null

Syntax Description

ipsec	Specifies that IP security (IPsec) authentication is used.
spi <*spi*>	Specifies the security parameter index (SPI). Valid range is **256** to **4294967295**.
md5 <*key*>	Specifies that MD5 authentication is used. Keys are specified in 32 hexadecimal characters.
sha1 <*key*>	Specifies that SHA-1 authentication is used. Keys are specified in 40 hexadecimal characters.
null	Specifies that no OSPFv3 authentication is used.

Default Values

By default, this is set to **null** (meaning no authentication is used).

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example specifies that no OSPFv3 authentication will be used on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 authentication null**

ospfv3 <*process id*> cost <*cost*>

Use the **ospfv3 cost** command to specify a value that represents the cost of sending an Open Shortest Path First version 3 (OSPFv3) packet over the interface. Use the **no** form of this command to return the cost to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
cost <*cost*>	Specifies the OSPFv3 cost of the interface. This value overrides any automatically computed cost value (default value). Valid range is **1** to **65535**.

Default Values

By default, the OSPFv3 cost of the interface is automatically computed. The automatic cost computation is the reference bandwidth divided by the interface bandwidth. The reference bandwidth is set by the command *auto-cost reference-bandwidth <value> on page 4150*, and defaults to **100** Mbps.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the OSPFv3 cost of the interface as **10**:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ospfv3 5 cost 10
```


ospfv3 <*process id*> dead-interval <*value*>

Use the **ospfv3 dead-interval** command to specify the maximum interval allowed between Open Shortest Path First version 3 (OSPFv3) Hello packets on the interface. If the maximum interval is exceeded, neighboring devices will assume that the device is down. This value must be the same across all interfaces on a link. Use the **no** form of this command to return the dead interval to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
dead-interval <*value*>	Specifies the maximum number of seconds allowed between OSPFv3 Hello packets. It is recommended that this value be **4** times the Hello packet interval (set with the command *ospfv3 <process id> hello-interval <value> on page 2290*). Valid range is **1** to **65535** seconds.

Default Values

By default, the maximum interval allowed between OSPFv3 Hello packets is set to **40** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To specify the dead interval between OSPFv3 Hello packets on the interface, enter the command as follows:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 5 dead-interval 100**

ospfv3 encryption

Use the **ospfv3 encryption** command to specify a symmetrical, bidirectional Open Shortest Path First version 3 (OSPFv3) security association (SA) that uses encapsulating security payload (ESP) for encryption and authentication of all OSPFv3 messages that are sent or received on the interface. This command allows you to specify OSPFv3 security at the interface level. Use the **no** form of this command to remove IP security (IPsec) protection of OSPFv3 messages on the interface. Variations of this command include:

ospfv3 encryption ipsec spi <*spi*> **esp** <*encryption type*> <*encryption key*> <*authentication type*> <*authentication key*>
ospfv3 encryption ipsec spi <*spi*> **esp null** <*authentication type*> <*authentication key*>
ospfv3 encryption null

Syntax Description

ipsec	Specifies that IPsec encryption is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by any other IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
esp	Specifies that ESP is used.
null	Specifies that OSPFv3 messages on this interface are not encrypted when used in the **ospfv3 encryption null** format (even when encryption is specified by the OSPFv3 area configuration). When used in the **ospfv3 encryption ipsec spi** <*spi*> **esp null** format, **null** indicates that messages on the interface will not be encrypted, but will be authenticated.
<*encryption type*>	Specifies the type of algorithm used to encrypt OSPFv3 messages. Valid values for encryption are: **3des** uses triple data encryption standard (DES). **aes-cbc** uses advanced encryption standard (AES) with cipher block chaining (CBC). Select from **aes-cbc 128**, **aes-cbc 192**, or **aes-cbc 256**. **des** uses DES.
<*encryption key*>	Specifies the hexadecimal encryption key. The size of the encryption key is determined by the respective encryption algorithm, as follows: **3des** uses a **48** character key size. **aes-cbc 128** uses a **32** character key size. **aes-cbc 192** uses a **48** character key size. **aes-cbc 256** uses a **64** character key size. **des** uses a **16** character key size.
<*authentication type*>	Specifies the algorithm used for authenticating OSPFv3 messages. Valid authentication methods are Message-Digest 5 (**md5**) and Secure-Hash 1 (**sha1**) algorithms.

<authentication key>	Specifies the hexadecimal authentication key. The size of the authentication key is determined by the respective authentication algorithm, as follows: **md5** uses a **32** character key size. **sha1** uses a **40** character key size.

Default Values

By default, there is no security for OSPFv3 messages on an interface.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

This commands specifies OSPFv3 security at the interface level. Protection specified with this command overrides any area-level OSPFv3 protection that might apply to the interface.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages with an SPI of **120**, no encryption, and **md5** as the authentication method:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 encryption ipsec spi 120 esp null md5 NeWtStpsswdLoonGpsswDhtThmnWoKEY**

ospfv3 <*process id*> **hello-interval** <*value*>

Use the **ospfv3 hello-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) Hello packets sent on the interface. This value must be the same across all interfaces on the link. Use the **no** form of this command to return the Hello packet interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
hello-interval <*value*>	Specifies the number of seconds allowed between OSPFv3 Hello packets. Valid range is **1** to **65535** seconds.

Default Values

By default, the Hello packet interval for OSPFv3 is **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the interval between OSPFv3 Hello packets on the interface is **20** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 5 hello-interval 20**

ospfv3 <*process id*> network

Use the **ospfv3 network** command to specify the network type for Open Shortest Path First version 3 (OSPFv3) enabled interfaces. Use the **no** form of this command to return the interface's network type to the default value. Variations of this command include:

ospfv3 <*process id*> **network broadcast**
ospfv3 <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
broadcast	Specifies that the OSPFv3 network type for the interface is set to broadcast.
point-to-point	Specifies that the OSPFv3 network type for the interface is set to point-to-point.

Default Values

By default, Ethernet interfaces are set to network type broadcast, and point-to-point (PPP), Frame Relay, and loopback interfaces are set to network type point-to-point.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the network interface as point-to-point:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 5 network point-to-point**

ospfv3 *<process id>* **priority** *<value>*

Use the **ospfv3 priority** command to specify the Open Shortest Path First version 3 (OSPFv3) priority for the interface. Use the **no** form of this command to return the interface's priority to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
priority *<value>*	Specifies the OSPFv3 priority for the interface. Valid range is **0** to **255**.

Default Values

By default, the OSPFv3 priority of an interface is set to **1**.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

Priority is used in the election of the designated router and backup designated router on multi-access networks. Interfaces connected to multi-access networks (such as Ethernet interfaces) perform an election for a designated and backup designated router. The router interface with the highest OSPFv3 priority on the link becomes the designated router for that link. The interface with the next highest priority becomes the designated backup router. In the event there is a tie, the router interface with the highest router ID takes precedence. A priority value of **0** indicates the router is ineligible to become either the designated or backup designated router.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's OSPFv3 priority value to **6**:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ospfv3 5 priority 6
```


ospfv3 <*process id*> retransmit-interval <*value*>

Use the **ospfv3 retransmit-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) sent on the interface. Use the **no** form of this command to return the OSPFv3 LSA interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
retransmit-interval <*value*>	Specifies the number of seconds between OSPFv3 LSAs sent on the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA retransmit interval is set to **5** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the LSA retransmit interval is **10** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 5 retransmit-interval 10**

ospfv3 <*process id*> shutdown

Use the **ospfv3 shutdown** command to disable an Open Shortest Path First version 3 (OSPFv3) process on the interface. When this command is used, the OSPFv3 commands remain in place, but logically it appears to the interface as though the OSPFv3 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv3 process.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables OSPFv3 process **5** on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 5 shutdown**

ospfv3 <*process id*> transmit-delay <*value*>

Use the **ospfv3 transmit-delay** command to specify the estimated time that is required to propagate an Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) on the interface. Use the **no** form of this command to return the transmit delay to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2283*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
transmit-delay <*value*>	Specifies the number of seconds required to send LSAs from the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA transmit delay is set to **1** second.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's LSA transmit delay to **2** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ospfv3 5 transmit-delay 2**

packet-capture <*name*>

Use the **packet-capture** command to apply a previously configured packet capture instance to the interface. Use the **no** form of this command to remove the packet capture instance.

Syntax Description

<*name*>	Specifies the name of the packet capture instance to apply to the interface.

Default Values

By default, no packet capture instances are configured or applied to the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. For more information about packet capturing, its uses, and its implementation in AOS, refer to the configuration guide *Configuring Packet Capture in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example applies the previously configured packet capture **1CAPTURE** to the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#packet-capture 1CAPTURE**

performance-statistics

Use the **performance-statistics** command to enable gathering performance monitoring statistics on the subinterface. Use the **no** form of this command to disable the performance monitoring feature.

Syntax Description

No subcommands.

Default Values

By default, performance monitoring is enabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables performance monitoring on the Ethernet subinterface **eth 0/1.1**:

(config)**#interface eth 0/1.1**
(config-eth 0/1.1)**#performance-statistics**

port-auth auth-mode

Use the **port-auth auth-mode** command to configure the authentication mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

port-auth auth-mode mac-based
port-auth auth-mode port-based
port-auth auth-mode port-based mac-auth-bypass
port-auth auth-mode voice-based
port-auth auth-mode voice-based mac-auth-bypass

Syntax Description

mac-based	Specifies a medium access control (MAC)-based authentication mode. Each host must authenticate separately.
port-based	Specifies a port-based authentication mode. Only a single host can participate in the authentication process.
voice-based	Specifies a voice-based authentication mode. Two hosts can participate in the authentication process: one in a voice virtual local area network (VLAN), and one in a data VLAN. A voice VLAN must be configured on the port for voice-based port authentication.
mac-auth-bypass	Optional. Specifies that if 802.1x authentication times out, the port will authenticate with a RADIUS server using the source MAC address. If the device connected to the port responds to 802.1x, MAC bypass will not be attempted.

Default Values

By default, the authentication mode is port based.

Command History

Release 10.1	Command was introduced.
Release 11.5.0	Command was expanded to include the **mac-auth-bypass** parameter.
Release R11.13.0	Command was expanded to include the **voice-based** parameter.

Usage Examples

The following example configures the unit for MAC-based authentication mode:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#port-auth auth-mode mac-based**

The following example configures the unit for voice-based authentication mode:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#port-auth auth-mode voice-based**

port-auth control-direction

Use the **port-auth control-direction** command to configure the direction in which traffic is blocked. This command is only applicable when authentication is port based. Use the **no** form of this command to return to the default setting. Variations of this command include:

port-auth control-direction both
port-auth control-direction in

Syntax Description

both	Blocks traffic in both directions when the port becomes unauthorized.
in	Blocks only incoming traffic when the port becomes unauthorized.

Default Values

By default, traffic is blocked in both directions.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example causes traffic to be blocked in both directions when the port becomes unauthorized:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#port-auth control-direction both**

port-auth guest-vlan <*vlan id*>

Use the **port-auth guest-vlan** command to configure guest virtual local area network (VLAN) for an interface. Use the **no** form of this command to return to the default setting.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Range is **1** to **4094**. If the specified VLAN does not exist, this command will create the VLAN.

Default Values

By default, no guest VLAN is configured.

Command History

Release 11.6.0	Command was introduced.

Functional Notes

Guest VLAN allows devices that fail authentication to be assigned to a predefined guest VLAN. For example, if a printer is plugged into a port and there is no RADIUS server to authenticate the new device or if RADIUS is not responding, the printer will be assigned to the guest VLAN and have network access granted to that VLAN.

Usage Examples

The following example configures the Ethernet interface 0/1 for guest VLAN **20**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#port-auth guest-vlan 20**

port-auth multiple-hosts

Use the **port-auth multiple-hosts** command to allow multiple hosts to access an authorized port without going through the authentication process. This command is only applicable when authentication is port based. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables multiple hosts to access an authorized port:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#port-auth multiple-hosts**

port-auth port-control

Use the **port-auth port-control** command to configure the port-authorization state. Use the **no** form of this command to return to the default setting. Variations of this command include:

port-auth port-control auto
port-auth port-control force-authorized
port-auth port-control force-unauthorized

Syntax Description

auto	Enables the port-authentication process.
force-authorized	Forces the port into an authorized state.
force-unauthorized	Forces the port into an unauthorized state.

Default Values

By default, all ports are forced to an authorized state.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example forces Ethernet port 0/1 into an unauthorized state:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#port-auth port-control force-unauthorized**

power inline

Use the **power inline** command to detect attached powered devices (PDs) and deliver 48 VDC, compliant with the IEEE 802.3af Power over Ethernet (PoE) standard, to the PD via existing CAT 5 cabling. To disable power detection and supply, use the **power inline never** command. Variations of this command include:

power inline auto
power inline legacy
power inline limit <*value*>
power inline never
power inline 2-point
power inline 4-point

Syntax Description

auto	Enables power detection and supply to PDs.
legacy	Enables power detection and supply of legacy non-IEEE 802.3af-compliant PDs.
limit <*value*>	Specifies the maximum amount of power that can be allocated to a PD connected to a specific port interface.
never	Disables power detection and supply to PDs.
2-point	Enables power detection and supply using the 2-point detection method necessary for some PDs.
4-point	Enables power detection and supply using the 4-point detection method necessary for some PDs. This method works consistently with LinkRunner 1000/200 devices when other detection methods fail.

Default Values

By default, PWR switches discover and provide power to IEEE-compliant PDs.

Command History

Release 9.1	Command was introduced.
Release A4.01	Command was expanded to include the **2-point** parameter.
Release R11.2.0	Command was expanded to include the **limit** parameter.
Release R12.2.0	Command was expanded to include the **4-point** parameter.

Functional Notes

The **power inline limit** <*value*> command specifies the maximum amount of power available for allocation on a particular port. When you set the limit using this command, the switch will use this value instead of the PD Classification to determine the amount of power that must be available before delivering power to a newly connected PD. If the total power available is greater than this setting, power will be delivered to the PD. In addition, if the PD ever tries to draw more power than this setting, power to the PD will be shut off.

The **power inline limit** <*value*> command is available only in AOS firmware version R11.2.0 and later, but the command is hidden and therefore does not provide any help text.

Usage Examples

The following example configures the Ethernet interface to detect and supply power to PDs:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#power inline auto**

The following example sets the maximum amount of power allocated to a PD on a Gigabit switchport interface to 12:

(config)**#interface gigabit-switchport 0/1**
(config-giga-swx 0/1)**#power inline limit 12**

qos

Use the **qos** (quality of service) command to set the interface to the trusted state and to set the default cost of service (CoS) value. To return to defaults, use the **no** form of this command. Variations of this command include:

qos default-cos <*value*>
qos trust cos

Syntax Description

default-cos <*value*>	Sets the default CoS value for untrusted ports and all untagged packets. Range is **0** through **7**.
trust cos	Sets the interface to the trusted state.

Default Values

By default, the interface is untrusted with a default CoS of **0**.

Command History

Release 5.1	Command was introduced.

Functional Notes

Set the interface to **trust cos** if received 802.1P. CoS values are considered valid (i.e., no need to reclassify) and do not need to be tagged with the default value. When set to untrusted, the **default-cos** value for the interface is used.

Usage Examples

The following example sets Ethernet interface 0/1 as a trusted interface and assigns untagged packets a CoS value of **1**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#qos trust cos**
(config-eth 0/1)**#qos default-cos 1**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair queue to use weighted fair queuing.
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example enables RTP quality monitoring on the Ethernet 0/2 interface:

(config)**#interface eth 0/2**
(config-eth 0/2)**#rtp quality-monitoring**

s-tag-dei

Use the **s-tag-dei** command to configure traffic egressing the interface to reflect the packet color, either green or yellow. Packets are colored by setting the Canonical Format Indicator/Discard Eligibility Indicator (CFI/DEI) bit in the S-TAG VLAN header. Green packets are set to 0, while yellow packets are set to 1. Use the **no** form of the command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example configures the egressing traffic on the Ethernet 0/2 interface to reflect the packet color in the S-TAG VLAN header:

```
(config)#interface eth 0/2
(config-eth 0/2)#s-tag-dei
```

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Us the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Usage Examples

The following example enables SNMP capability on the Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#no snmp trap link-status**

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** command to enable or disable the bridge protocol data unit (BPDU) filter on a specific interface. This setting overrides the related global setting (refer to *spanning-tree edgeport bpdufilter default on page 1835*). Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree bpdufilter disable
spanning-tree bpdufilter enable

Syntax Description

disable	Disables BPDU filter for this interface.
enable	Enables BPDU filter for this interface.

Default Values

By default, this setting is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpdufilter blocks any BPDUs from being transmitted and received on an interface.

Usage Examples

The following example enables the BPDU filter on the Ethernet interface 0/3:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree bpdufilter enable**

The BPDU filter can be disabled on the Ethernet interface 0/3 by issuing the following commands:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree bpdufilter disable**

spanning-tree bpduguard

Use the **spanning-tree bpduguard** command to enable or disable the bridge protocol data unit (BPDU) guard on a specific interface. This setting overrides the related global setting (refer to *spanning-tree forward-time <value> on page 1839*). Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree bpduguard disable
spanning-tree bpduguard enable

Syntax Description

disable	Disables BPDU guard for this interface.
enable	Enables BPDU guard for this interface.

Default Values

By default, this setting is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpduguard blocks any BPDUs from being received on an interface.

Usage Examples

The following example enables the BPDU guard on the interface Ethernet interface 0/3:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree bpduguard enable**

The BPDU guard can be disabled on the Ethernet interface 0/3 by issuing the following commands:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree bpduguard disable**

spanning-tree cost <*value*>

Use the **spanning-tree cost** command to assign a cost to the interface. The cost value is used when computing the spanning-tree root path. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies a cost value of **1** to **200000000**.

Default Values

By default, the cost value is set to **1000** Mbps.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the interface to a path cost of **1200**:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree cost 1200**

spanning-tree edgeport

Use the **spanning-tree edgeport** command to enable or disable the interface as an edgeport. This command overrides the related global setting (refer to *spanning-tree edgeport default on page 1837*). Variations of this command include:

spanning-tree edgeport disable
spanning-tree edgeport enable

Syntax Description

disable	Specifies that the interface is not an edgeport.
enable	Specifies that the interface is an edgeport.

Default Values

By default, this setting is disabled.

Command History

Release 5.1	Command was introduced.
Release 8.1	Command was added to the ATM subinterface command set.
Release R10.1.0	Command was expanded to include the **disable** and **enable** keywords.

Functional Notes

When an interface is designated as an edgeport, the interface will immediately go into a forwarding state when the link becomes active. When an interface is not designated as an edgeport, the interface must progress through the listening and learning states before going to the forwarding state.

Usage Examples

The following example specifies that the interface is an edgeport:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#spanning-tree edgeport enable**

The following example disables the interface as an edgeport:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#spanning-tree edgeport disable**

spanning-tree link-type

Use the **spanning-tree link-type** command to configure the spanning tree protocol link type for each interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared

Syntax Description

auto	Determines link type by the port's duplex settings.
point-to-point	Manually sets link type to **point-to-point** regardless of duplex settings.
shared	Manually sets link type to **shared** regardless of duplex settings.

Default Values

By default, the interface is set to auto.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command overrides the default link type setting determined by the duplex of the individual port. By default, a port configured for half-duplex is set to **shared** link type, and a port configured for full-duplex is set to **point-to-point** link type. Setting the link type manually overrides the default and forces the port to use the specified link type. Use the **link-type auto** command to restore the convention of determining link type based on duplex settings.

Usage Examples

The following example forces the link type to **point-to-point**, even if the port is configured to be half-duplex:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree link-type point-to-point**

Technology Review

Rapid transitions are possible in Rapid Spanning Tree Protocol (RSTP) by taking advantage of point-to-point links (a port is connected to exactly one other bridge) and edge-port connections (a port is not connected to any additional bridges). Setting the link type to **auto** allows the spanning tree to automatically configure the link type based on the duplex of the link. Setting the link type to **point-to-point** allows a half-duplex link to act as if it were a point-to-point link.

spanning-tree path-cost *<value>*

Use the **spanning-tree path-cost** command to assign a cost to a bridge group that is used when computing the spanning-tree root path. To return to the default path-cost value, use the **no** form of this command.

Syntax Description

<value>	Assigns a number to the bridge interface to be used as the path cost in spanning calculations. Valid range is **0** to **65535**.

Default Values

By default, the path-cost value is set to **19**.

Command History

Release 1.1	Command was introduced.
Release 8.1	Command was added to the ATM subinterface command set.
Release R10.1.0	Command was added to the Ethernet interface command set.

Functional Notes

The specified value is inversely proportional to the likelihood the bridge interface will be chosen as the root path. Set the path-cost value lower to increase the chance the interface will be the root. To obtain the most accurate spanning-tree calculations, develop a system for determining path costs for links and apply it to all bridged interfaces.

Usage Examples

The following example assigns a path cost of 100 on an Ethernet interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#spanning-tree path-cost 100**

Technology Review

Spanning-tree protocol provides a way to prevent loopback or parallel paths in bridged networks. Using the priority values and path costs assigned to each bridging interface, the spanning-tree protocol determines the root path and identifies whether to block or allow other paths.

spanning-tree pathcost method

Use the **spanning-tree pathcost method** command to select a short or long method used by the spanning-tree protocol. Variations of this command include:

spanning-tree pathcost method long
spanning-tree pathcost method short

Syntax Description

long	Specifies 32-bit values when calculating pathcosts.
short	Specifies 16-bit values when calculating pathcosts.

Default Values

By default, **spanning-tree pathcost method** is set to **short**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example specifies that the spanning tree protocol use a long pathcost method:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree pathcost method long**

spanning-tree port-priority <*value*>

Use the **spanning-tree port-priority** command to select the priority level of this interface. To return to the default setting, use the **no** form of this command.

Syntax Description

<*value*>	Specifies a priority-level value from **0** to **240** (this value must be in increments of 16).

Default Values

By default, this set to **128**.

Command History

Release 5.1	Command was introduced.

Functional Notes

The only time that this priority level is used is when two interfaces with a path to the root have equal cost. At that point, the level set in this command will determine which port the spanning tree will use. Set the priority value lower to increase the chance the interface will be used.

Usage Examples

The following example sets the interface to a priority of **100**:

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#spanning-tree port-priority 100**

spanning-tree rootguard

Use the **spanning-tree rootguard** command to enable or disable the root guard on a specific interface. This setting overrides the related global setting (refer to *spanning-tree edgeport rootguard default on page 1838*). Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree rootguard disable
spanning-tree rootguard enable

Syntax Description

disable	Disables root guard for this interface.
enable	Enables root guard for this interface.

Default Values

By default, this setting is disabled.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Root guard blocks an interface from being elected to the root port role. If information about a superior root bridge is received, the interface will no longer forward traffic until superior root bridge proposals stop. If an interface has bridge protocol data unit (BPDU) filter or BPDU guard configured, configuring root guard will have no effect on the operation of the interface. The root guard setting can be overridden on an individual port basis.

Usage Examples

The following example enables the root guard on the gigabit switchport interface 0/3:

(config)**#interface gigabit-switchport 0/3**
(config-giga-swx 0/3)**#spanning-tree rootguard enable**

The following example disables the root guard on the gigabit switchport interface 0/3:

(config)**#interface gigabit-switchport 0/3**
(config-giga-swx 0/3)**#spanning-tree rootguard disable**

speed

Use the **speed** command to configure the speed of an Ethernet interface. Use the **no** form of this command to return to the default value. Variations of this command include:

speed 10
speed 100
speed 1000
speed 1000 nonegotiate
speed 2500
speed 10000
speed auto

Syntax Description

10	Specifies 10 Mbps Ethernet.
100	Specifies 100 Mbps Ethernet.
1000	Specifies 1 Gbps Ethernet. This only applies to Gigabit Ethernet interfaces.
2500	Specifies 2.5 Gbps Ethernet. This only applies to Gigabit Ethernet interfaces.
10000	Specifies 10 Gbps Ethernet. This only applies to 10 Gigabit Ethernet interfaces.
nonegotiate	Optional. Specifies that auto-negotiation is disabled on Gigabit Ethernet interfaces that use a fiber medium.
auto	Automatically detects 10 or 100 Mbps Ethernet and negotiates the duplex setting.

Some Ethernet equipment (though rare) is unable to negotiate duplex if speed is manually determined. To avoid incompatibilities, manually set the duplex if the speed is manually set. Refer to ethernet-cfm mep on page 2175 and half-duplex on page 2185.

Default Values

By default, speed is set to **auto**.

Command History

Release 1.1	Command was introduced.
Release 17.5	Command was expanded to include the **2500** Mbps parameter.
Release R10.10.0	Command was expanded to include the **10000** Mbps parameter.
Release R12.1.0	Command was made unavailable for Ethernet interfaces on virtual AOS (vAOS) instances.

Functional Notes

This command is not available for Ethernet interfaces on vAOS instances.

Usage Examples

The following example configures the Ethernet port for **100** Mbps operation:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#speed 100**

storm-control action shutdown

Use the **storm-control action shutdown** command to shut down the interface when a storm occurs. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled; the interface will only filter traffic.

Command History

Release 5.1	Command was introduced.

Functional Notes

Enabling this option shuts down the interface if a multicast, unicast, or broadcast storm occurs.

Usage Examples

The following example shuts down Ethernet interface 0/1 if a storm is detected:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#storm-control action shutdown**

storm-control level

Use the **storm-control level** command to configure limits on the rates of broadcast, multicast, and unicast traffic on a port. Use the **no** form of this command to disable this feature. Variations of this command include:

storm-control broadcast level *<rising level>*
storm-control broadcast level *<rising level> <falling level>*
storm-control multicast level *<rising level>*
storm-control multicast level *<rising level> <falling level>*
storm-control multicast-broadcast level ***<rising level>***
storm-control unicast level *<rising level>*
storm-control unicast level *<rising level> <falling level>*

Syntax Description

broadcast level	Sets levels for broadcast traffic.
multicast level	Sets levels for multicast traffic.
multicast-broadcast level	Sets levels for multicast and broadcast traffic.
unicast level	Sets levels for unicast traffic.
<rising level>	Specifies a rising level, which determines the percentage of total bandwidth the port accepts before it begins blocking packets. Range is **1** to **100** percent.
<falling level>	Optional. Specifies a falling level, which determines when the storm is considered over, causing AOS to no longer block packets. This level must be less than the rising level. Range is **1** to **100** percent.

Default Values

By default, **storm-control** is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

This setting configures the rising and falling suppression values. When the selected rising level (which is a percentage of total bandwidth) is reached, the port begins blocking packets of the specified type (i.e., broadcast, multicast, or unicast). AOS uses the rising level as its falling level if no falling level is specified.

Availability of this command and its variations will differ across AOS platforms.

Usage Examples

The following example sets the rising suppression level to **85** percent for multicast packets:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#storm-control multicast level 85**

The following example sets the rising suppression level to **80** percent for broadcast packets, with a falling level of **50** percent:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#storm-control broadcast level 80 50**

storm-control rate

Use the **storm-control rate** command to configure maximum ingress data rates for broadcast, unknown multicast, and unknown unicast traffic on a switch port. Use the **no** form of this command to disable the feature. Variations of this command include:

storm-control broadcast rate <*rate*>
storm-control broadcast rate <*rate*> **burst** <*size*>
storm-control multicast-unknown rate <*rate*>
storm-control multicast-unknown rate <*rate*> **burst** <*size*>
storm-control unicast-unknown rate <*rate*>
storm-control unicast-unknown rate <*rate*> **burst** <*size*>

Syntax Description

broadcast	Specifies the maximum data rate for all ingress broadcast traffic.
multicast-unknown	Specifies the maximum data rate for ingress unknown multicast traffic.
unicast-unknown	Specifies the maximum data rate for ingress unknown unicast traffic.
rate <*rate*>	Specifies the maximum ingress data rate in Kilobytes per second. Valid range is **64** to **33554368** Kbps.
burst <*size*>	Optional. Specifies the maximum traffic burst (in bytes) of the specified traffic type that can ingress the port. Valid selections are **4K**, **16K**, **64K**, **256K**, **1M**, **4M**, **8M**, and **16M** bytes.

Default Values

By default, storm control is disabled. When enabled, the burst size is set to **64K** bytes by default.

Command History

Release R11.8.0	Command was introduced.

Functional Notes

Storm control is used to lessen the impacts of traffic flooding on certain ports.

Address Resolution Protocol (ARP), Dynamic Host Control Protocol (DHCP), and other protocols commonly use broadcasts, so setting the broadcast storm control rate too low can adversely impact these protocols in an otherwise healthy network.

The configured multicast storm control rate applies only to multicast traffic with addresses not learned by Internet Group Management Protocol (IGMP) snooping.

Unknown unicast traffic usually exist only for initial traffic to a client or traffic sent to a client that was unlearned or that timed out. Setting the unicast storm control rate too low can impact traffic to clients that actually exist but are temporarily unknown to the switch. Spanning tree topology change notifications (TCNs) clear the known unicast addresses on some ports of the switch and cause all unicast traffic from these clients to be unknown until the addresses are relearned. This behavior can cause the temporary rate of unknown unicast frames to spike. Switching networks that have relatively static topologies should use the spanning tree edge-port setting to limit spanning tree TCNs so that a lower storm control unicast rate can be set. If the network topology changes frequently, a larger unicast storm control rate should be set so that traffic is not adversely impacted after a spanning tree TCN.

All traffic is received on switchports at full line rate, meaning that the momentary rate of received traffic will almost always exceed any storm control rate configured lower than the port's linked rate. The configured burst size determines how many bytes can burst over the configured rate before storm control makes a decision to begin dropping traffic for a configured traffic type. A smaller storm control burst size causes the rate to be imposed on received frames earlier in the storm of undesired frames. Setting a higher burst rate is less likely to drop frames in case of many back-to-back frames, but also exposes the network to more of the initial frames of a storm of undesired frames. Once a burst is exhausted, it takes an interval of time to refill completely. This interval, in seconds, is defined as the (burst rate * 8)/rate.

When a switchport is part of a port channel, storm control settings are not allowed on the switchport. Rather, storm control rate and burst settings are only allowed on the port channel of which the switchport is a member.

Usage Examples

The following example configures broadcast traffic storm control with a rate of **1000** Kbps and the default burst size:

(config)**#interface xgigabit-switchport 1/1**
(config-xgiga-swx 1/1)**#storm-control broadcast rate 1000**

subtended-host mode

Use the **subtended-host mode** command to enable or disable subtended host listening on the interface. This command allows the interface to receive pre-provisioning information from another AOS unit. Variations of this command include:

subtended-host mode listener
subtended-host mode disabled

Syntax Description

listener	Enables the interface to receive pre-provisioning information from another unit.
disabled	Disables the interface from receiving any pre-provisioning information from another unit.

Default Values

By default, the first configured MEF Ethernet interface has pre-provisioning listening enabled. In addition, the Gigabit Ethernet interface **0/1** and EFM group **1/1** interfaces have pre-provisioning listening enabled by default. Any additional interfaces have pre-provisioning listening disabled.

Command History

Release A4.05	Command was introduced.
Release R11.1.0	Command was expanded to include the Gigabit Ethernet and EFM group interfaces.

Functional Notes

Only one interface at a time can have the subtended-host mode set to **listener**. If all interfaces have a subtended-host mode of **disabled**, then all pre-provisioning information is discarded.

Usage Examples

The following example enables the Ethernet interface 0/1 to receive subtended-host provisioning:

(config)**#interface ethernet 0/1**
(config-ethernet 0/1)**#subtended-host mode listener**

switchport access vlan <*vlan id*>

Use the **switchport access vlan** command to set the port to be a member of the virtual local area network (VLAN) when in access mode. To reset the port to be a member of the default VLAN, use the **no** form of this command.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Range is **1** to **4094**.

Default Values

By default, this is set to VLAN **1** (the default VLAN).

Command History

Release 5.1	Command was introduced.

Functional Notes

If the port is in the trunk mode, this command will not alter the switchport mode to access. Instead it will save the value to be applied when the port does switch to access mode. Refer to *switchport mode on page 2331* for more information.

Usage Examples

The following example sets the switchport mode to static access and makes the Ethernet interface 0/1 port a member of VLAN **2**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport mode access**
(config-eth 0/1)**#switchport access vlan 2**

switchport gvrp

Use the **switchport gvrp** command to enable or disable GARP VLAN Registration Protocol (GVRP) on an interface. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, GVRP is disabled on all ports.

Command History

Release 8.1	Command was introduced.

Functional Notes

Enabling GVRP on any interface enables GVRP globally.

Usage Examples

The following example enables GVRP on Ethernet interface 0/24:

(config)**#interface ethernet 0/24**
(config-eth 0/24)**#switchport gvrp**

switchport mode

Use the **switchport mode** command to configure the virtual local area network (VLAN) membership mode. Use the **no** form of this command to reset membership mode to the default value. Variations of this command include:

switchport mode access
switchport mode activchassis
switchport mode stack
switchport mode trunk

Syntax Description

access	Sets port to be a single (nontrunked) port that transmits and receives no tagged packets.
activchassis	Sets the port to allow it to communicate with other ActivChassis devices.
stack	Sets the port to allow it to communicate with a switch stack.
trunk	Sets port to transmit and receive packets on all VLANs included in its VLAN allowed list.

Default Values

By default, on non-ActivChassis devices, the **switchport mode** is set to **access**. By default, on ActivChassis-enabled devices, the **switchport mode** is set to **activchassis**.

Command History

Release 5.1	Command was introduced.
Release AC1.0	Command was expanded to include the **activchassis** parameter.

Functional Notes

Configuring the interface for stack mode (using the **switchport mode stack** command) enables the switch to communicate with other switches that are capable of stacking.

- If the switch is configured as the stack master (using the (config)**#stack master** command), it will begin advertising itself as a stack master.
- If the switch is configured as the stack member (using the (config)**#stack member** command), it will begin advertising other stack masters that it knows about.

Stack mode also allows the port to transmit and receive packets on all VLANs that are included in the VLAN allowed list.

In ActivChassis mode, the switchport becomes part of the ActivChassis backplane, and it is not available to connect to devices outside of the ActivChassis. The port must be directly connected to other devices with the same capability and settings. In addition, if the port is part of the ActivChassis backplane, and it currently has an active link, the port mode cannot be changed from **activchassis** mode. For more information about configuring ActivChassis, refer to the configuration guide *Configuring ActivChassis in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example sets the port to be a **trunk** port:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport mode trunk**

The following example changes the port function on a device with ActivChassis enabled:

(config)**#interface xgigabit-switchport 1/1**
(config-xgiga-swx 1/1)**#switchport mode activchassis**

switchport port-security

Use the **switchport port-security** command to enable port security functionality on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

This command is disabled by default.

Command History

Release 8.1	Command was introduced.

Functional Notes

You cannot enable port security on a port that is already configured as the following:

- Monitor session destination
- Member of a port channel interface
- Dynamic or trunk port (i.e., the port must be configured as static access)

Usage Examples

The following example enables port security on the Ethernet interface 0/1 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport port-security**

switchport port-security aging

Use the **switchport port-security aging** command to enable and configure secure medium access control (MAC) address aging on a particular interface. Use the **no** form of this command to disable this feature. Variations of this command include:

switchport port-security aging static
switchport port-security aging time <*value*>
switchport port-security aging type absolute

Syntax Description

static	Configures the interface to age static, as well as dynamic entries in the secure MAC address table.
time <*value*>	Enables port security aging for dynamic entries in the secure MAC address table by configuring a time (in minutes). Disable aging by setting the time to 0.
type absolute	Configures the address to be removed after the specified time regardless of activity.

Default Values

By default, dynamic and static aging are disabled.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example sets the aging time of secure MAC addresses to **10** minutes:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport port-security aging time 10**

switchport port-security expire

Use the **switchport port-security expire** command to disable an interface after a specified amount of time. Use the **no** form of this command to return to the default setting. Variations of this command include:

switchport port-security expire time <*value*>
switchport port-security expire type absolute

Syntax Description

time <*value*>	Enables port expiration by configuring a time (in minutes). Disable by setting time to 0.
type absolute	Configures the interface to shut down after the specified time regardless of activity.

Default Values

By default, this command is disabled and set to **type absolute**.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example disables Ethernet interface 0/1 after **10** minutes:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport port-security expire time 10**

switchport port-security mac-address

Use the **switchport port-security mac-address** command to add a static secure medium access control (MAC) address or sticky secure MAC address associated with the interface and to enable sticky address learning. Use the **no** form of this command to remove a MAC address associated with this port. Variations of this command include the following:

switchport port-security mac-address <*mac address*>
switchport port-security mac-address <*mac address*> **vlan** <*vlan id*>
switchport port-security mac-address sticky
switchport port-security mac-address sticky-volatile
switchport port-security mac-address sticky <*mac address*>
switchport port-security mac-address sticky <*mac address*> **vlan** <*vlan id*>

Syntax Description

sticky	Optional. Enables sticky address learning if no MAC address is specified. The learned addresses persist across a reboot.
sticky-volatile	Optional. Enables sticky address learning for the immediate session only. The learned addresses do not appear in the configuration and do not persist across a reboot.
<*mac address*>	Optional. Adds a MAC address associated with this interface. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
vlan <*vlan id*>	Optional. Associates the MAC address with the specified VLAN. VLAN ID range is **1** to **4094**.

Default Values

By default, sticky learning is disabled and there are no configured MAC addresses.

Command History

Release 8.1	Command was introduced.
Release 17.4	Command was expanded to include the **sticky-volatile** parameter.
Release 17.9	Command was expanded to include the **vlan** parameter.

Functional Notes

For more information about port security configuration, refer to the configuration guide *Configuring Port Access Control in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example adds a single static address and enables sticky address learning on interface Ethernet interface 0/1:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport port-security mac-address 00:A0:C8:02:D0:30**
(config-eth 0/1)**#switchport port-security mac-address sticky**

switchport port-security maximum <*value*>

Use the **switchport port-security maximum** command to configure the maximum number of secure medium access control (MAC) addresses associated with the interface. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the maximum number of secure MAC addresses to be associated with the interface. Range is **1** to **132**.

Default Values

The default value for this command is **1**.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example sets the maximum supported MAC addresses for Ethernet interface 0/1 to **2**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport port-security maximum 2**

switchport port-security violation

Use the **switchport port-security violation** command to configure the action to be taken once a security violation is encountered. Use the **no** form of this command to return to the default setting. Variations of this command include:

switchport port-security violation protect
switchport port-security violation restrict
switchport port-security violation shutdown

Syntax Description

protect	Determines that the unit will not learn any new secure addresses (nor allow these new sources to pass traffic) until the number of currently active secure addresses drops below the maximum setting.
restrict	Determines that the security violation counter increments and an Simple Network Management Protocol (SNMP) trap is sent once a violation is detected. The new address is not learned and data from that address is not allowed to pass.
shutdown	Determines that the interface is disabled once a violation is detected. A **no shutdown** command is required to re-enable the interface.

Default Values

The default for this command is shutdown.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example configures the interface to react to security violations by not learning the addresses and not accepting data from the violation source:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport port-security violation restrict**

switchport protected

Use the **switchport protected** command to prevent the port from transmitting traffic to all other protected ports. A protected port can only send traffic to unprotected ports. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

This command is disabled by default.

Command History

Release 10.1	Command was introduced.

Usage Examples

In the example below, all three of the ports are on virtual local area network (VLAN) 3, and Ethernet 0/1 and Ethernet 0/2 are designated as protected ports. Ethernet 0/3 is unprotected. Ethernet 0/1 and Ethernet 0/2 will be allowed to send traffic to Ethernet 0/3, but traffic traveling between Ethernet 0/1 and Ethernet 0/2 will be blocked.

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport access vlan 3**
(config-eth 0/1)**#switchport protected**
(config-eth 0/1)**#exit**

(config)**#interface ethernet 0/2**
(config-eth 0/2)**#switchport access vlan 3**
(config-eth 0/2)**#switchport protected**
(config-eth 0/2)**#exit**

(config)**#interface ethernet 0/3**
(config-eth 0/3)**#switchport access vlan 3**

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** command to allow certain virtual local area networks (VLANs) to transmit and receive traffic on this port when the interface is in trunking mode. To return to defaults, use the **no** form of this command. Variations of this command include:

switchport trunk allowed vlan <*list*>
switchport trunk allowed vlan add <*list*>
switchport trunk allowed vlan all
switchport trunk allowed vlan except <*list*>
switchport trunk allowed vlan none
switchport trunk allowed vlan remove <*list*>

Syntax Description

<*list*>	Specifies a list of valid VLAN interface IDs. Refer to *Functional Notes* below.
add	Adds the specified VLAN IDs to the VLAN trunking allowed list.
all	Adds all configured VLAN IDs to the VLAN trunking allowed list.
except	Adds all configured VLAN IDs to the VLAN trunking allowed list except those specified in the <*vlan id list*>.
none	Adds no VLAN IDs to the VLAN trunking allowed list.
remove	Removes VLAN IDs from the VLAN trunking allowed list.

Default Values

By default, all valid VLANs are allowed.

Command History

Release 5.1	Command was introduced.

Functional Notes

A VLAN list is a set of VLAN IDs delimited by commas. A valid VLAN ID value must be from **1** through **4094**. A range of IDs may be expressed as a single element by using a hyphen between endpoints. For example, the VLAN ID range **1,2,3,4,6,7,8,9,500** may be more easily expressed as **1-4,6-9,500**. No spaces are allowed in a valid ID range.

Usage Examples

The following example adds VLANs to the previously existing list of VLANs allowed to transmit and receive on this port:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport trunk allowed vlan add 1-4,6-9,500**

switchport trunk fixed vlan

Use the **switchport trunk fixed vlan** command to change the configured list of virtual local area networks (VLANs) that remain fixed in use only when GARP VLAN Registration Protocol (GVRP) is enabled on the interface. Of these VLANs, VLANs statically created will be available for use on the interface. Use the **no** form of this command to disable this feature. Variations of this command include:

switchport trunk fixed vlan add <*list*>
switchport trunk fixed vlan all
switchport trunk fixed vlan except <*list*>
switchport trunk fixed vlan none
switchport trunk fixed vlan remove <*list*>

Syntax Description

<*list*>	Specifies a list of valid VLAN interface IDs. Refer to *Functional Notes* below.
add	Adds VLANs to the VLAN GVRP trunking fixed list.
all	Adds all VLANs to the VLAN GVRP trunking fixed list.
except	Adds all VLAN IDs to the VLAN trunking fixed list except those in the command line VLAN ID list.
none	Removes all VLANs from the VLAN GVRP trunking fixed list.
remove	Removes VLAN from the VLAN trunking fixed list.

Default Values

By default, no VLANs are in the VLAN GVRP trunking fixed list (**switchport trunk fixed vlan none**).

A VLAN list is a set of VLAN IDs delimited by commas. A valid VLAN ID value must be from **1** through **4094**. A range of IDs may be expressed as a single element by using a hyphen between endpoints. For example, the VLAN ID range **1,2,3,4,6,7,8,9,500** may be more easily expressed as **1-4,6-9,500**. No spaces are allowed in a valid ID range.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command has no effect on VLAN membership configuration unless GVRP is enabled on the interface.

Usage Examples

The following example changes the configured list of fixed VLANs by adding VLAN **50** to the list.

(config-eth 0/20)**#switchport trunk fixed vlan add 1-15,25-30,40**
(config-eth 0/20)**#switchport trunk fixed vlan add 50**

The following example changes the configured list of fixed VLANs by removing VLANs 10 to 100 from the list:

(config-eth 0/20)**#switchport trunk fixed vlan remove 10-100**

The following example changes the configured list of fixed VLANs to include only VLANs 1 to 1000:

(config-eth 0/20)**#switchport trunk fixed vlan 1-1000**

The following example changes the configured list of fixed VLANs to include no VLANs (except those VLANs that are native):

(config-eth 0/20)**#switchport trunk fixed vlan none**

switchport trunk native vlan <*vlan id*>

Use the **switchport trunk native vlan** command to set the virtual local area network (VLAN) native to the interface when the interface is in trunking mode. To return to defaults, use the **no** form of this command.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Range is **1** to **4094**.

Default Values

By default, this is set to VLAN **1**.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configure which VLAN the interface uses as its native VLAN during trunking. Packets from this VLAN leaving the interface will not be tagged with the VLAN number. Any untagged packets received by the interface are considered a part of the native VLAN ID.

Usage Examples

The following example sets the native VLAN on Ethernet interface 0/1 to VLAN **2**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#switchport trunk native vlan 2**

switchport vlan

Use the **switchport vlan** command to create a Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) network policy that specifies a virtual local area network (VLAN) for **voice**, **guest-voice**, **softphone**, or **voice-signalling** applications. Use the optional **cos** and **dscp** keywords to define class of service (CoS) and differentiated services code point (DSCP) values associated with the application. Use the **no** form of this command to remove an existing network policy. Variations of this command include:

switchport guest-voice vlan <*vlan id*>
switchport guest-voice vlan <*vlan id*> **[cos** <*value*> **| dscp** <*value*> **| cos** <*value*> **dscp** <*value*>**]**
switchport softphone vlan <*vlan id*>
switchport softphone vlan <*vlan id*> **[cos** <*value*> **| dscp** <*value*> **| cos** <*value*> **dscp** <*value*>**]**
switchport voice vlan <*vlan id*>
switchport voice vlan <*vlan id*> **[cos** <*value*> **| dscp** <*value*> **| cos** <*value*> **dscp** <*value*>**]**
switchport voice-signalling vlan <*vlan id*>
switchport voice-signalling vlan <*vlan id*> **[cos** <*value*> **| dscp** <*value*> **| cos** <*value*> **dscp** <*value*>**]**

Syntax Description

guest-voice	Specifies a guest voice application, which is used to define a policy for guest users with a limited feature set voice service.
softphone	Specifies a softphone application, which is used to define a policy for softphone applications that operate on devices, such as PCs or laptop computers.
voice	Specifies a voice application, which is used to define a policy for dedicated IP phone handsets and other similar devices supporting interactive voice services.
voice-signalling	Specifies a voice signaling application, which is used to define a policy for the command and control signaling that supports voice and guest voice applications.
<*vlan id*>	Specifies the voice VLAN ID. Range is **1** to **4094**.
cos <*value*>	Optional. Specifies the CoS value assigned to the application. Range is **0** to **7**.
dscp <*value*>	Optional. Specifies the DSCP value assigned to the application. Range is **0** to **63**.

Default Values

By default, no LLDP-MED network policies are configured.

If an application and VLAN are specified without the optional CoS or DSCP parameters, then default CoS and DSCP values are assigned.

Default CoS values are: **voice** (5); **voice-signalling** (3); **guest-voice** (0); **softphone** (0).

Default DSCP values are: **voice** (46); **voice-signalling** (26); **guest-voice** (0); **softphone** (0).

Command History

Release 16.1	The command **switchport voice vlan** <*vlan id*> was introduced.
Release 17.2	Command was expanded to include the additional applications: **guest-voice**, **softphone**, and **voice-signalling**. The optional **cos** and **dscp** parameters were added.

Functional Notes

The switchport command allows a configured interface to function as an access point (AP) for a VLAN while adding the specified VLAN to the port's allowed VLAN list. This command automatically sets the port to spanning tree edgeport mode, but this mode is not automatically reset when the voice, guest voice, softphone, or signaling VLAN is removed.

If the VLAN specified in this command does not yet exist, it will be created in Adtran Operating System (AOS) when the command is issued.

A network policy is typically configured on switchport interfaces in AOS devices that support LLDP-MED. An exception is the NetVanta 1524ST, where network policies are configured on Gigabit Ethernet interfaces.

At least one network policy should be configured on a switchport interface that is connected to an LLDP-MED capable endpoint. Depending on the type and use of Voice over Internet Protocol (VoIP) equipment attached to the switchport interface, multiple network policies may need to be configured on the same interface.

Some endpoints prefer to use untagged VLANs for their application. To achieve this in AOS, configure the application to be on the same VLAN of which the port is a member. By default, this is VLAN 1.

For more information about allowed VLAN lists, refer to switchport trunk allowed vlan on page 2341. For more information about spanning-tree edgeport mode, refer to spanning-tree edgeport on page 2315. For more information about switchport mode, refer to switchport mode on page 2331.

Usage Examples

The following example establishes a voice network policy that uses VLAN **200**.

(config)**#interface switchport 0/1**
(config-swx 0/1)**#switchport voice vlan 200**

Since CoS and DSCP values are not specified in the above network policy, the default values for voice applications will be used: CoS (5); DSCP (46).

The following example establishes a voice network policy that uses VLAN 200 with CoS priority set to **4** and DSCP priority set to **36**.

(config)**#interface switchport 0/1**
(config-swx 0/1)**#switchport voice vlan 200 cos 4 dscp 36**

traffic-shape rate <*value*>

Use the **traffic-shape rate** command to specify and enforce an output bandwidth for Ethernet and virtual local area network (VLAN) interfaces. Variations of this command include:

traffic-shape rate <*value*>
traffic-shape rate <*value*> **count-eth-overhead**
traffic-shape rate <*value*> <*burst*>
traffic-shape rate <*value*> <*burst*> **count-eth-overhead**

Syntax Description

<*value*>	Specifies the rate (in bits per second) at which the interface should be shaped.
<*burst*>	Optional. Specifies the allowed burst in bytes. By default, the burst is specified as the rate divided by 5 and represents the number of bytes that would flow within 200 ms.
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.

Default Values

By default, traffic-shaping rate is disabled.

Command History

Release 10.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the **count-eth-overhead** parameter, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

Traffic shaping can be used to limit an Ethernet segment to a particular rate or to specify use of quality of service (QoS) on Ethernet or VLAN interfaces.

Usage Examples

The following example sets the outbound rate of Ethernet interface 0/1 to 128 kbps and applies a QoS policy that gives all Realtime Transport Protocol (RTP) traffic priority over all other traffic:

(config)**#qos map voip 1**
(config-qos-map)**#match ip rtp 10000 10500 all**
(config-qos-map)**#priority unlimited**
(config-qos-map)**#interface ethernet 0/1**
(config-eth 0/1)**#traffic-shape rate 128000**
(config-eth 0/1)**#qos-policy out voip**

vlan-id <*vlan id*>

Use the **vlan-id** command to set a virtual local area network (VLAN) ID for the Ethernet interface. Use the **no** form of this command to remove an entry. Variations of this command include:

vlan-id <*vlan id*>
vlan-id <*vlan id*> **native**

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID number. Range is **1** to **4095**.
native	Optional. Specifies that data for that VLAN ID goes out untagged. If **native** is not specified, data for that VLAN ID goes out tagged.

Default Values

By default, no VLAN ID is set.

Command History

Release 6.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.

Usage Examples

The following example configures a native VLAN of 5 for the Ethernet interface 0/1:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vlan-id 5 native**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the Ethernet interface 0/1 to the VRF instance named **RED**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrf forwarding RED**

vrrp <*number*>

Use the **vrrp** command to configure Internet Protocol version 4 (IPv4) Virtual Router Redundancy Protocol version 2 (VRRPv2) routers within a router group. Use the **no** form of this command to remove the VRRP router's configurations. Variations of this command include:

vrrp <*number*> **description** <*text*>
vrrp <*number*> **ip** <*ipv4 address*>
vrrp <*number*> **ip** <*ipv4 address*> **secondary**
vrrp <*number*> **preempt**
vrrp <*number*> **preempt delay minimum** <*time*>
vrrp <*number*> **priority** <*level*>
vrrp <*number*> **shutdown**
vrrp <*number*> **startup-delay** <*delay*>
vrrp <*number*> **timers advertise** <*interval*>
vrrp <*number*> **timers learn**
vrrp <*number*> **track** <*name*>
vrrp <*number*> **track** <*name*> **decrement** <*value*>

Syntax Description

<*number*>	Specifies the VRRP router group's virtual router ID (VRID) number. Range is **1** to **255**.
description <*text*>	Specifies the textual description of the VRRP router within the group.
ip <*ipv4 address*>	Specifies the IPv4 address to be used by the VRRP router. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
secondary	Optional. Specifies the entry of an additional VRRP router supported IPv4 address.
preempt	Allows a VRRP router to preempt the current master router if its priority level is higher than the current master's.
delay minimum <*time*>	Optional. Specifies a delay (in seconds) before the specified router will attempt to preempt the current master router. Range is **0** to **255** seconds.
priority <*level*>	Specifies the configured priority level of the VRRP router. Range is **1** to **254**.
shutdown	Disables the VRRP router.
startup-delay <*delay*>	Specifies a time delay (in seconds) before a VRRP router becomes active. Range is **0** to **255** seconds.
timers	Specifies the configuration of the VRRP timers.
advertise <*interval*>	Specifies the time (in seconds) between advertisements sent by the master router. Range is **1** to **255** seconds.
learn	Specifies that the backup VRRP router learns the advertisement interval of the master router.
track <*name*>	Specifies a change in priority level of the VRRP router based upon the specified track.
decrement <*value*>	Optional. Specifies the numerical amount to decrement the VRRP's priority level if the track transitions to a FAIL state. Range is **1** to **254**.

Default Values

By default, VRRP is enabled.

By default, a VRRP router will preempt with no additional delay.

The default configured priority for a VRRP router that is either a backup router or not the IP address owner is **100**. The default actual priority of a VRRP router that is the IP address owner is **255**.

By default, startup-delay is enabled with a default value of **35** seconds.

By default, the advertisement interval is **1** second.

By default, the default decrement value is **10**.

Command History

Release 16.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.

Functional Notes

A VRRP router may be part of more than one virtual router group. Although VRRP group VRIDs can be numbered between 1 and 255, only two VRRP routers per interface are supported.

Adtran recommends that the **timers advertise** setting is kept at the default value. If it is necessary to change this setting, ensure that all VRRP routers are configured with the new value, as all VRRP routers in the virtual group must have the same advertisement interval value. It is also recommended that if the **timers learn** function is enabled on one router in a virtual router group, then the **timers learn** function should be enabled on all routers in the group.

When the virtual router's specified IPv4 address is independent of the IPv4 addresses assigned to real interfaces on the VRRP routers, there is no IPv4 address owner. This addressing method is preferred if object tracking will be used to monitor the network connection. The IPv4 address used for the virtual router must be on the same subnet as either the primary or secondary IPv4 addresses assigned to the VRRP router's real interface.

A track must be created before the **vrrp track** command can be issued. Refer to the *Network Monitor Track Command Set on page 4098* for more information on creating tracks. If a VRRP router owns the virtual router IP address, then the VRRP router's priority level cannot be decremented as a result of the track command. If object tracking will be used, it is important that no VRRP router own the virtual router IP address.

Usage Examples

The following example describes a VRRP router within virtual router group **1** as the **Default Master Router**:

(config)**#interface eth 0/1**
(config-eth 0/1)**#vrrp 1 description Default Master Router**

The following example specifies an IPv4 address of **10.0.0.1** for a VRRP router within virtual router group **1**:

(config)**#interface eth 0/1**
(config-eth 0/1)**#vrrp 1 ip 10.0.0.1**

The following example specifies that the VRRP router within virtual router group **1** preempts the current master router after a **30** second delay:

(config)**#interface eth 0/1**
(config-eth 0/1)**#vrrp 1 preempt delay minimum 30**

The following example specifies the configured priority for the VRRP router within virtual router group **1** is **254**:

(config)**#interface eth 0/1**
(config-eth 0/1)**#vrrp 1 priority 254**

The following example disables the VRRP router within virtual router group **1**:

(config)**#interface eth 0/1**
(config-eth 0/1)**#vrrp 1 shutdown**

The following example configures a VRRP router on group **1** to delay **45** seconds before becoming active:

(config)**#interface eth 0/1**
(config-eth 0/1)**#vrrp 1 startup-delay 45**

vrrpv3 <*vrid*> address-family

Use the **vrrpv3 address-family** command to configure Virtual Router Redundancy Protocol version 3 (VRRPv3) routers on the interface. This command enables VRRPv3, creates a virtual router ID (VRID), and specifies whether you are using Internet Protocol version 4 (IPv4) or IP version 6 (IPv6) VRRPv3. Use the **no** form of this command to remove the VRRPv3 router configuration. Variations of this command include:

vrrpv3 <*vrid*> **address-family ipv4**
vrrpv3 <*vrid*> **address-family ipv6**

Syntax Description

<*vrid*>	Specifies the VRID for the virtual router instance. This value is advertised by VRRPv3 and is used to generate the virtual router medium access control (MAC) address. Valid range is **1** to **255**.
ipv4	Specifies that IPv4 is used with VRRPv3, and enters the virtual router instance's configuration mode.
ipv6	Specifies that IPv6 is used with VRRPv3, and enters the virtual router instance's configuration mode.

Default Values

By default, VRRPv3 is not configured.

Command History

Release R10.11.0	Command was introduced. This command replaces **vrrpv3** <*vrid*> on the interface.

Functional Notes

VRID values must be the same on all routers that are part of the virtual router group. VRID numbering is independent between VRRPv3 IPv4 and IPv6 address families. Once the VRRPv3 VRID is created and the address family is specified, the virtual router instance's configuration mode is entered. Only two VRIDs per interface per IP version are supported. For more information about configuring the VRRPv3 instance, refer to *VRRPv3 Command Set on page 4221*.

Usage Examples

The following example enables IPv4 VRRPv3, creates a VRID of **15** for the instance, and enters the virtual router instance's configuration mode:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#vrrpv3 15 address-family ipv4
(config-if-vrrpv3 15)#
```


The following example enables IPv6 VRRPv3, creates a VRID of **6** for the instance, and enters the virtual router instance's configuration mode:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 6 address-family ipv6**
(config-if-vrrpv3 6)#

vxlan tunnel <*interface id*> vni <*number*>

Use the **vxlan tunnel** <*interface id*> **vni** <*number*> command to associate the interface with a virtual extensible local area network (VxLAN) tunnel interface and VxLAN network ID (VNI). Use the **no** form of this command to return to the default setting.

Syntax Description

<interface id>	Specifies the VxLAN interface ID number. Valid range is **1** to **1024**.
<number>	Specifies the VNI number to which this interface is mapped. Valid range is **1** to **677215**.

Default Values

By default, an Ethernet interface is not associated with a VxLAN tunnel interface or a VNI.

Command History

Release R13.1.0	Command was introduced.

Functional Notes

Two Ethernet interfaces cannot be associated with the same VxLAN tunnel interface or VNI. If the VxLAN tunnel needs to be protected with virtual private network (VPN), an IP security (IPSec) profile must be applied to the tunnel using the command *tunnel protection ipsec profile <name> on page 3349***.** When 802.1q encapsulation is enabled, VxLAN can only be configured on Ethernet subinterfaces.

Usage Examples

The following example associates Ethernet interface 0/1 with VxLAN tunnel interface **3** and VNI **2**:

(config)**#interface ethernet 0/1**
(config-eth-0/1)**#vxlan tunnel 3 vni 2**

FDL INTERFACE COMMAND SET

FDL Interface Configuration mode is used for establishing a Telnet session over the FDL (facility data link). To activate, enter the **interface fdl** command and specify the associated slot/port number (of the T1 interface used) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface fdl 1/1
(config-fdl 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

ip address <ipv4 address> <subnet mask> on page 2358
ip address range <start ipv4 address> <end ipv4 address> <subnet mask> secondary on page 2359
ip learn-address on page 2360
ip mtu <size> on page 2361
peer default ip address <ipv4 address> on page 2363

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 7.1	Command was introduced for the facility data link (FDL) interface.
Release R10.1.0	Command was expanded to include the **secondary** keyword.

Usage Examples

The following example configures an IPv4 address of **192.22.72.101 /30**:

(config)**#interface fdl 1/1**
(config-fdl 1/1)**#ip address 192.22.72.101 /30**

ip address range *<start ipv4 address> <end ipv4 address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface fdl 1/1**
(config-fdl 1/1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip learn-address

Use the **ip learn-address** command to automatically learn the IP address of the remote unit. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables the facility data link (FDL) to automatically learn the remote unit's IP address:

(config)**#interface fdl 1/1**
(config-fdl 1/1)**#ip learn-address**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface fdl 1/1**
(config-fdl 1/1)**#ip mtu 1200**

peer default ip address *<ipv4 address>*

Use the **peer default ip address** command to specify the default Internet Protocol version 4 (IPv4) address of the remote end of this interface. Use the **no** form of this command to remove a default IP address.

Syntax Description

<ipv4 address>	Specifies the default IPv4 address for the remote end. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there is no assigned peer default IPv4 address.

Command History

Release 3.1	Command was introduced.
Release 7.1	Command was expanded to include the facility data link (FDL).

Functional Notes

This command is useful if the peer's FDL interface is on a different subnet than the local unit's FDL interface IPv4 address. This is common if the FDL interface is unnumbered to another interface's IPv4 address.

Usage Examples

The following example sets the default peer IPv4 address to **192.22.71.50**:

(config)**#interface fdl 1/1**
(config-fdl 1/1)**#peer default ip address 192.22.71.50**

FXO INTERFACE COMMAND SET

To activate the Foreign Exchange Office (FXO) Interface Configuration mode, enter the **interface fxo** command and specify the FXO port at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface fxo 0/1
(config-fxo 0/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

impedance on page 2365
loopback on page 2366
rx-gain <value> on page 2367
test erl on page 2368
test loop on page 2370
test ring-ground on page 2371
test tip-ground on page 2372
test tone on page 2373
tx-gain <value> on page 2374

impedance

Use the **impedance** command to configure the alternating current (AC) impedance of the 2-wire interface. Use the **no** form of this command to return to the default value. Variations of this command include:

impedance [600c | 900r]
impedance [900c | 600r]
impedance bt3
impedance [z1| z2 | z3 | z4 | z5 | z6 | z7]

Syntax Description

600c	Specifies an impedance of 600 Ω **+** 2.16 µF.
600r	Specifies an impedance of 600 Ω real.
900c	Specifies an impedance of 900 Ω + 2.16 µF.
900r	Specifies an impedance of 900 Ω real.
bt3	Specifies an impedance of Rs 370 ohms, Rp 620 ohms, Cp 310nF
z1	Specifies an impedance of Rs 220 W, Rp 820 W, Cp 115 nF.
z2	Specifies an impedance of Rs 270 W, Rp 750 W, Cp 150 nF.
z3	Specifies an impedance of Rs 270 W, Rp 750 W, Cp 150 nF, Zin 600r.
z4	Specifies an impedance of Rs 320 W, Rp 1050 W, Cp 230 nF.
z5	Specifies an impedance of Rs 350 W, Rp 1000 W, Cp 210 nF, Zin 600r.
z6	Specifies an impedance of Rs 370 W, Rp 620 W, Cp 310 nF.
z7	Specifies an impedance of Rp 800 W, Rs 100 W, Cs 50 nF.

Default Values

By default, the impedance is set to **600c**.

Command History

Release 7.1	Command was introduced.
Release A1	Command was expanded to include the settings **z1** through **z7**.
Release 14.2.0	Command was expanded to include the setting bt3

Usage Examples

The following example sets the impedance to 600 Ω + 2.16 µF:

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#impedance 600c**

loopback

Use the **loopback** command to activate a loopback on the foreign exchange office (FXO) module. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback analog
loopback digital

Syntax Description

analog	Initiates a loopback toward the T1 network side of the connection after passing through analog filters in the voice CODEC.
digital	Initiates the same loopback before passing through analog filters in the voice coder-decoder (CODEC).

Default Values

No default values are necessary for this command.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example activates a loopback toward the T1 network side of the connection after passing through analog filters in the voice CODEC:

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#loopback analog**

rx-gain <*value*>

Use the **rx-gain** command to define the receive gain characteristics on the foreign exchange office (FXO) interface. Receive gain determines the amplification of the received signal before transmitting it out the FXO interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Defines the receive gain characteristics for the interface in 0.1 decibel increments. Range is **-6.0** to **10.0** dB.

Default Values

By default, this command is set to **0** dB.

Command History

Release 7.1	Command was introduced.

Functional Notes

When increasing this value, the signal being received on this port sounds louder. When decreasing this value, the signal being received on this port sounds softer.

Usage Examples

The following example defines the receive gain as **-5.4** dB:

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#rx-gain -5.4**

test erl

Use the **test erl** command to automatically determine the correct impedance value for analog lines connected to the foreign exchange office (FXO) port. This is helpful when troubleshooting problems with FXO equipment and assists in adjusting the correct audio levels. Use the **no** form of the **test erl all** and **test erl current** command to disable these features. Variations of this command include:

test erl all
test erl all auto-set
test erl clear-results
test erl current
test erl display-results

*This feature is available only on units with digital signal processor (DSP) hardware version Freescale MSC7119, and AOS version A2.02 or above. To determine the DSP hardware version, issue the **show version** command and look for the DSP hardware version.*

Syntax Description

all	Specifies running the test repeatedly, testing all available impedance settings for the interface.
auto-set	Optional. Sets automatically the best measured impedance for the interface.
clear-results	Clears the results from the echo return loss (erl) test.
current	Specifies running the test once, using the current impedance setting.
display-results	Displays a snapshot of the current test status.

Default Values

By default, this command is disabled.

Command History

Release A2.04	Command was introduced.

Functional Notes

Before using this feature, an analog line from the service provider must be connected to the FXO interface and the line must be idle (no call in progress). The FXO interface must be connected to a voice trunk in order to make the tool available for use.

During the test, the tool sets the FXO transmit gain and receive gain levels to 0 dB to make the proper measurements. These settings are returned to the configured values when the test is complete. The rx-gain value adjusts the level being transmitted from the FXO to the line. The tx-gain value adjusts the level being transmitted from the FXO to the dsp.

Common low ERL values are between 5 and 8 dB. Acceptable ERL values begin around 12 dB. The higher the ERL value, the more gain adjustment can be made without introducing echo. The commonly recommended configuration is a receive gain of 0 dB and a transmit gain of +6 dB.

The following is an error that could result by attempting to measure ERL when a measurement sequence is already active:

```
% could not run erl test
```

During test execution, a warning is issued when a test sequence terminates abnormally. Reasons for early termination include:

- Was not able to seize the line
- Line disconnected during test
- DSP timeout (i.e., when the DSP hardware version does not support this feature)
- Test runs for more than 20 seconds per impedance value (for example, 80 seconds with a 4 impedance setting)

Usage Examples

The following example tests the FXO interface 0/1 to automatically find the best measured impedance settings:

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#test erl all auto-set**

The following example displays the ERL test status (the output is shown after the command):

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#test erl display-results**

Port	Impedance	Status	Measured ERL
fxo 0/1	600 c		10 dB
fxo 0/1	900 r		8 dB
fxo 0/1	900 c		9 dB
fxo 0/1	z1		13 dB
fxo 0/1	z2		11 dB
fxo 0/1	z3		14 dB
fxo 0/1	z4		12 dB
fxo 0/1	z5	test calling	

test loop

Use the **test loop** command to manually control the foreign exchange office (FXO) interface's hook switch. This is helpful when troubleshooting problems with the FXO equipment. Use the **no** form of this command to disable this feature. Variations of this command include:

test loop closed
test loop open

Syntax Description

closed	Closes the hook switch, allowing DC current to flow through the interface.
open	Opens the hook switch, preventing DC current from flowing through the interface.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example opens the interface's hook switch:

(config)**#interface fxo 02/1**
(config-fxo 0/1)**#test loop open**

test ring-ground

Use the **test ring-ground** command to force the ring conductor to ground potential and provides battery on tip for detection of tip ground. This is helpful when troubleshooting problems with ground start (GS) circuits. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example forces a ring-ground test of the foreign exchange office (FXO) interface:

```
(config)#interface fxo 0/1
(config-fxo 0/1)#test ring-ground
```

test tip-ground

Use the **test tip-ground** command to detect the removal of the ring ground and check for the loop condition on an active foreign exchange office (FXO) interface. This is helpful when troubleshooting problems with ground start (GS) circuits. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example forces a tip-ground test of the FXO interface:

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#test tip-ground**

test tone

Use the **test tone** command to activate the 1 kHz test tone. Use the **no** form of this command to deactivate the test tone. Variations of this command include:

test tone far
test tone near

Syntax Description

far	Sends the test tone out the T1 network interface to the remote end.
near	Sends the test tone toward the foreign exchange office (FXO) interface.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sends the test tone toward the FXO interface:

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#test tone near**

tx-gain <*value*>

Use the **tx-gain** command to define the transmit gain characteristics on the foreign exchange office (FXO) interface. Transmit gain determines the amplification of the transmitted signal before transmitting from the FXO interface toward the network. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Defines the transmit gain characteristics in 0.1 decibel increments. Range is **-6.0** to **10.0** dB.

Default Values

By default, transmit gain is set to **0** dB.

Command History

Release 7.1	Command was introduced.

Functional Notes

When increasing this value, the signal being transmitted to the far end sounds louder. When decreasing this value, the signal being transmitted to the far end sounds softer.

Usage Examples

The following example defines the transmit gain as **-5.4** dB on the FXO interface:

(config)**#interface fxo 0/1**
(config-fxo 0/1)**#tx-gain -5.4**

FXS INTERFACE COMMAND SET

To activate the Foreign Exchange Station (FXS) Interface Configuration mode, enter the **interface fxs** command and specify the FXS port at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface fxs 2/1
(config-fxs 2/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

battery-mode on page 2376
caller-id on page 2377
holdover <value> on page 2378
impedance on page 2379
loopback on page 2381
onhook-transmission on page 2382
ring-frequency <value> on page 2383
ring-voltage <value> on page 2384
rx-gain <value> on page 2385
signal on page 2386
test commands begin on page 2387
tx-gain <value> on page 2393

battery-mode

Use the **battery-mode** command to configure the battery that feeds the foreign exchange station (FXS) loop. Use the **no** form of this command to return to the default setting. Variations of this command include:

battery-mode auto
battery-mode high
battery-mode low

Syntax Description

auto	Configures the interface to automatically switch between high and low battery.
high	Configures the interface to only use the high battery.
low	Configures the interface to only use the low battery.

Default Values

By default, the battery mode is set to **auto**.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example configures the battery mode for **high**:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#battery-mode high**

caller-id

Use the **caller-id** command to configure caller identification (ID). Use the **no** form of this command to cancel the setting. Variations of this command include:

caller-id delay <*value*>
caller-id format mdmf
caller-id format sdmf

Syntax Description

delay <*value*>	Specifies the delay between ring-off and caller ID frequency-shift keying (FSK). Valid range is **500** to **2000** ms. Common values are 500, 750, and 1000.
format	Specifies the format for caller ID as **mdmf** or **sdmf**.
mdmf	Indicates the caller ID format as multiple data message format (mdmf).
sdmf	Indicates the caller ID format as single data message format (sdmf).

Default Values

By default, caller ID is disabled.

Command History

Release A2	Command was introduced.

Usage Examples

The following example configures the caller ID delay to **500** ms:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#caller-id delay 500**

holdover *<value>*

Use the **holdover** command to configure the amount of time (in seconds) to sustain battery power at the foreign exchange station (FXS) port even if a call could not be connected. Once the holdover period has expired, the power is removed from the FXS port. A value of **0** will result in the battery being maintained at the FXS indefinitely. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the time (in seconds) to apply power from the battery to the FXS port. Valid range is **0** to **65535** seconds.

Default Values

The default value for this command is **60** seconds.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example configures the holdover to **25** seconds:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#holdover 25**

impedance

Use the **impedance** command to configure the alternating current (AC) impedance of the 2-wire interface. Use the **no** form of this command to return to the default value. Variations of this command include:

impedance 600c
impedance 600r
impedance 900b
impedance 900c
impedance 900r
impedance z1
impedance z2
impedance z3
impedance z4
impedance z5
impedance z6
impedance z7

Syntax Description

600c	Specifies an impedance of 600 Ω **+** 2.16 µF.
600r	Specifies an impedance of 600 Ω real.
900b	Use only when directed by Adtran and only with part number 1203602L1.
900c	Specifies an impedance of 900 Ω + 2.16 µF.
900r	Specifies an impedance of 900 Ω real.
z1	Specifies an impedance of Rs 220 W, Rp 820 W, Cp 115 nF.
z2	Specifies an impedance of Rs 270 W, Rp 750 W, Cp 150 nF.
z3	Specifies an impedance of Rs 270 W, Rp 750 W, Cp 150 nF, Zin 600r.
z4	Specifies an impedance of Rs 320 W, Rp 1050 W, Cp 230 nF.
z5	Specifies an impedance of Rs 350 W, Rp 1000 W, Cp 210 nF, Zin 600r.
z6	Specifies an impedance of Rs 370 W, Rp 620 W, Cp 310 nF.
z7	Specifies an impedance of Rp 800 W, Rs 100 W, Cs 50 nF.

Default Values

The default value for this command is **600r**.

Command History

Release 6.1	Command was introduced.
Release A1	Command was expanded to include the **900b** impedance setting.
Release A2	Command was expanded to include the **z1** impedance setting.
Release A4.03	Command was expanded to include the **z2**, **z3**, **z4**, **z5**, **z6**, and **z7** impedance settings.

Usage Examples

The following example sets the impedance to 600 Ω + 2.16 μF:

>**enable**
#**configure terminal**
(config)#**interface fxo 0/1**
(config-fxo 0/1)#**impedance 600c**

loopback

Use the **loopback** command to activate a loopback toward the T1 network side on the foreign exchange station (FXS) module. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback analog
loopback digital

Syntax Description

analog	Initiates a loopback toward the T1 network side of the connection after passing through analog filters in the voice coder-decoder (CODEC).
digital	Initiates the same loopback before passing through analog filters in the voice CODEC.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example activates a loopback toward the T1 network side of the connection after passing through analog filters in the voice CODEC:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#loopback analog**

onhook-transmission

Use the **onhook-transmission** command to configure the on-hook transmission of voice band audio on the foreign exchange station (FXS) interface. Use the **no** form of this command to return to the default value. Variations of this command include:

onhook-transmission always
onhook-transmission auto

Syntax Description

always	Enables on-hook transmission of voice band audio.
auto	Enables on-hook transmission of voice band audio when it is possible. This option lowers the power consumption of the unit; however, it should not be used if voice message waiting indication is enabled on the port.

Default Values

By default, on-hook transmission is set to **always**.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the on-hook transmission to **auto**:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#onhook-transmission auto**

ring-frequency *<value>*

Use the **ring-frequency** command to change the ring frequency of a single foreign exchange service (FXS) port from the default system country value. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the FXS port ring frequency. Valid values are **20**, **25**, and **50** Hz.

Default Values

By default, the command *voice system-country <name> on page 1970* automatically configures the appropriate FXS port ring frequency for the specified country. Below is a list of the default ring frequencies (in Hertz) for fully-supported countries:

Australia	25 Hz	Mexico	25 Hz
Belgium	25 Hz	Puerto Rico	20 Hz
Canada	20 Hz	United Arab Emirates	25 Hz
ETSI	25 Hz	United Kingdom	25 Hz
Ireland	25 Hz	United States	20 Hz

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example configures the ring frequency for FXS port **2/1** as **25** Hz**.**

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#ring-frequency 25**

ring-voltage <*value*>

The **ring-voltage** command sets the ring voltage for the foreign exchange station (FXS) interface. Increasing the ring voltage, sends a stronger ring signal to the phones connected to this interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies a ring voltage. Select from **50**, **60** or **70** Vrms.

Default Values

By default, ring voltage is set to **50** Vrms.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sets the ring voltage to **60** Vrms:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#ring-voltage 60**

rx-gain <*value*>

Use the **rx-gain** command to define the receive gain characteristics on the foreign exchange station (FXS) interface. Receive gain determines the amplification of the received signal before transmitting out the FXS interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Defines the receive gain characteristics for the interface in 0.1 decibel increments. Range is **-12.0** to **6.0** dB.

Default Values

By default, this command is set to **-3.0** dB.

Command History

Release 6.1	Command was introduced.

Functional Notes

When increasing this value, the signal being received on this port sounds louder. When decreasing this value, the signal being received on this port sounds softer.

Usage Examples

The following example defines the receive gain as **-6.4** dB:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#rx-gain -6.4**

signal

The **signal** command configures the signaling mode for the foreign exchange station (FXS) interface. Use the **no** form of this command to return to the default value. Variations of this command include:

signal ground-start
signal loop-start

Syntax Description

ground-start	Applies resistance to the tip conductor of the circuit to indicate an off-hook condition.
loop-start	Bridges the tip and ring to indicate an off-hook (seizing the line) condition.

Default Values

By default, this command is set to **loop-start**.

Command History

Release 6.1	Command was introduced.

Functional Notes

This signaling mode must match the configuration of the network.

Usage Examples

The following example sets the signaling mode to **loop-start**:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#signal loop-start**

test battery

Use the **test battery** command to provide battery on the 2-wire foreign exchange station (FXS) interface. This is helpful when troubleshooting wiring problems with the FXS equipment. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example provides battery on the 2-wire FXS interface:

```
(config)#interface fxs 2/1
(config-fxs 2/1)#test battery
```

test line

The **test line** command performs GR-909 line tests including the Hazardous Potential Test, the Foreign ElectroMotive Force Test, the Resistive Faults Test, the Receiver-Off-Hook Test, and the Ringers Test on the foreign exchange station (FXS) interface.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example runs GR-909 line tests on the FXS interface:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#test line**

test reverse-battery

Use the **test reverse-battery** command to provide reverse battery polarity on the foreign exchange station (FXS) interface. This is helpful when troubleshooting wiring problems with the FXS equipment. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example provides reverse battery polarity on the FXS interface:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#test reverse-battery**

test ringing

Use the **test ringing** command to activate ringing voltage on the 2-wire foreign exchange station (FXS) interface (using a 2-seconds-on/4-seconds-off cadence). The **no** form of this command removes the ringing voltage from the interface.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example activates ringing voltage on the 2-wire FXS interface:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#test ringing**

test tip-open

Use the **test tip-open** command to provide battery on ring and a high impedance on tip. This is helpful when troubleshooting problems with ground start (GS) interfaces. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example provides battery on ring and a high impedance on tip on the foreign exchange station (FXS) interface:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#test tip-open**

test tone

Use the **test tone** command to activate the 1 kHz test tone. Use the **no** form of this command to deactivate the test tone. Variations of this command include:

test tone near
test tone far

Syntax Description

near	Sends the test tone toward the foreign exchange station (FXS) interface.
far	Sends the test tone out the T1 network interface to the remote end.

Default Values

By default, this command is disabled.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sends the test tone toward the FXS interface:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#test tone near**

tx-gain <*value*>

Use the **tx-gain** command to define the transmit gain characteristics (configured in 0.1 dB increments) on the foreign exchange station (FXS) interface. Transmit gain determines the amplification of the received signal before transmitting from the FXS interface toward the network. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Defines the transmit gain characteristics for the interface in 0.1 decibel increments. Range is **-12.0** to **6.0** dB.

Default Values

By default, this command is set to **-6.0** dB.

Command History

Release 6.1	Command was introduced.

Functional Notes

When increasing this value, the signal being transmitted to the far end will sound louder. When decreasing this value, the signal being transmitted to the far end sounds softer.

Usage Examples

The following example defines the transmit gain as **-6.4** dB on the FXS interface:

(config)**#interface fxs 2/1**
(config-fxs 2/1)**#tx-gain -6.4**

G.703 INTERFACE COMMAND SET

To activate the G.703 Interface Configuration mode, enter the **interface e1** command (and specify the G.703 port) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface e1 1/2
(config-e1 1/2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

coding on page 2395
framing crc4 on page 2396
loopback network on page 2397
snmp trap link-status on page 2398
test-pattern on page 2399
ts16 on page 2400

coding

Use the **coding** command to configure the line coding for the G.703 physical interface. This setting must match the line coding supplied on the circuit by the private branch exchange (PBX). Use the **no** form of this command to return to the default setting. Variations of this command include:

coding ami
coding hdb3

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
hdb3	Configures the line coding for high-density bipolar 3 (HDB3).

Default Values

By default, all E1 interfaces are configured with HDB3 line coding.

Command History

Release 5.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the E1 circuit. A mismatch will result in line errors (e.g., bipolar violations (BPVs)).

Usage Examples

The following example configures the G.703 interface for AMI line coding:

(config)**#interface e1 1/2**
(config-e1 1/2)**#coding ami**

framing crc4

Use the **framing crc4** command to configure the framing format for the G.703 interface. This parameter should match the framing format set on the external device. Use the **no** form of this command to return to the default value.

Syntax Description

crc4	Enables CRC4 bits to be transmitted in the outgoing data stream. Also, the received signal is checked for CRC4 errors.

Default Values

By default, CRC4 is enabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The framing value must match the configuration of the E1 circuit. A mismatch will result in a loss of frame alarm.

Usage Examples

The following example configures the G.703 interface for CRC4 framing:

(config)**#interface e1 1/2**
(config-e1 1/2)**#framing crc4**

loopback network

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback network line
loopback network payload

Syntax Description

line	Initiates a metallic loopback of the physical E1 network interface.
payload	Initiates a loopback of the E1 framer (CSU portion) of the E1 network interface.

Default Values

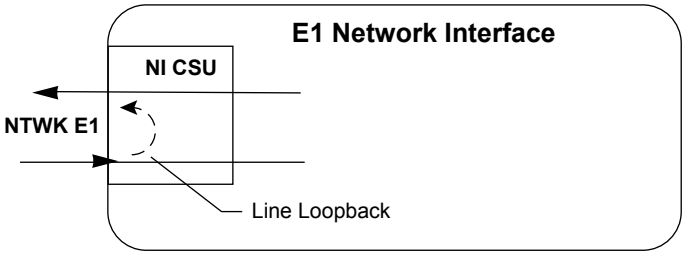
No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

The following diagram depicts a line loopback.



Usage Examples

The following example initiates a line loopback of the G.703 interface:

(config)**#interface e1 1/2**
(config-e1 1/2)**#loopback network line**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the G.703 interface:

(config)**#interface e1 1/2**
(config-e1 1/2)**#no snmp trap link-status**

test-pattern

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation. Variations of this command include:

test-pattern ones
test-pattern zeros

Syntax Description

ones	Generates a test pattern of continuous ones.
zeros	Generates a test pattern of continuous zeros.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.
Release 6.1	Command was expanded to include the E1 and G.703 interfaces.

Usage Examples

The following example activates the pattern generator for a stream of continuous **ones**:

(config)**#interface e1 1/2**
(config-e1 1/2)**#test-pattern ones**

ts16

Use the **ts16** command to enable timeslot 16 multiframe to be checked on the receive signal. Use the **no** form of this command to disable timeslot 16.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables timeslot **16** multiframing:

```
(config)#interface e1 1/2
(config-e1 1/2)#ts16
```

HSSI INTERFACE COMMAND SET

To activate the High Speed Serial Interface (HSSI) Interface Configuration mode, enter the **interface hssi** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface hssi 1/1
(config-hssi 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

external-loopback-request on page 2402
loopback on page 2403
snmp trap link-status on page 2404

external-loopback-request

Use the **external-loopback-request** command to enable LC (loopback circuit C) input to control loopbacks toward the network. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables the unit to accept external loopback requests:

(config)**#interface hssi 1/1**
(config-hssi 1/1)**#external-loopback-request**

loopback

Use the **loopback** command to initiate or remove a loopback. Use the **no loopback** command to disable all loopbacks. Variations of this command include:

loopback dce
loopback dte
loopback line
loopback remote
loopback none

Syntax Description

dce	Initiates a loopback on the data communication equipment (DCE).
dte	Initiates a loopback on the data terminal equipment (DTE).
line	Initiates a local line loopback.
remote	Initiates a remote line loopback.
none	Removes an active loopback.

Default Values

By default, no loopbacks are active.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example initiates a local **line** loopback on the high speed serial interface (HSSI):

(config)**#interface hssi 1/1**
(config-hssi 1/1)**#loopback line**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the interface:

(config)**#interface hssi 1/1**
(config-hssi 1/1)**#no snmp trap link-status**

MODEM INTERFACE COMMAND SET

To activate the Modem Interface Configuration mode, enter the **interface modem** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface modem 1/2
(config-modem 1/2)#
```

> *The modem interface number in the example above is shown as **modem 1/2**. This number is based on the interface's location (slot/port) and could vary depending on the unit's configuration. Use the **do show interfaces** command to determine the appropriate interface number.*

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

caller-id override on page 2406
dialin on page 2407
ignore-ring on page 2408
init-string <string> on page 2409
resource pool-member on page 2410

caller-id override

Use the **caller-id override** command to configure the unit to replace caller ID information with a user-specified number. Use the **no** form of this command to disable any caller ID overrides. Variations of this command include:

caller-id override always <*number*>
caller-id override if-no-cid <*number*>

Syntax Description

always <*number*>	Always forces replacement of the incoming caller ID number with the number given.
if-no-cid <*number*>	Replaces the incoming caller ID number with the number given only if there is no caller ID information available for the incoming call.

Default Values

By default, this command is disabled.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command forces a replacement of the incoming caller ID number with the number given. The received caller ID, if any, is discarded, and the given override number is used to connect the incoming call to a circuit of the same number.

Usage Examples

The following example configures the unit to always provide the given number as the caller ID number:

(config)**#interface modem 1/2**
(config-modem 1/2)**#caller-id override always 5555555**

dialin

Use the **dialin** command to enable the modem for remote console dial in, disabling the use of the modem for dial backup. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **dialin** is disabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example enables remote console dial in:

(config)**#interface modem 1/2**
(config-modem 1/2)**#dialin**

ignore-ring

Use the **ignore-ring** command to ignore incoming call ring events for the modem. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, **ignore-ring** is disabled.

Command History

Release R14.3	Command was introduced.

Usage Examples

The following example configures the modem to ignore incoming call ring events:

(config)**#interface modem 1/2**
(config-modem 1/2)**#ignore-ring**

init-string *<string>*

Use the **init-string** command to specify an initialization string for the modem using standard AT commands. Use the **no** form of this command to return to the default initialization string.

Syntax Description

<string>	Specifies an initialization string using standard AT commands. This string must start with AT and cannot contain spaces.

Default Values

<string>	**ate0q0v1x4\n0**	
	at	All initialization strings must begin with AT.
	e0	Disables command echo.
	q0	Response messages on.
	v1	Formats result codes in long word form.
	x4	Specifies extended response set, dial tone, and busy signal detection for result codes following modem operations.
	\n0	Selects standard buffered connection only.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example configures the modem to perform a hang-up at each initialization (to verify that the line is free) and maintains the default initialization:

(config)**#interface modem 1/2**
(config-modem 1/2)**#init-string ate0q0v1x4\n0**

resource pool-member

Use the **resource pool-member** command to assign the interface to a resource pool, making it a demand routing resource. Use the **no** form of this command to return to the default value. Variations of this command include:

resource pool-member <*name*>
resource pool-member <*name*> <*cost*>

Syntax Description

<*name*>	Specifies the name of the resource pool to which this interface is assigned.
<*cost*>	Optional. Specifies the cost of using this resource interface within the specified pool. In the event of a tie, a resource with a lower cost will be selected first. Interfaces with the same cost will be selected in alphabetical order by interface name.

Default Values

By default, the interface is not assigned to any resource pool.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures a basic rate interface (BRI) as a member of resource pool **MyPool**:

(config)**#interface modem 1/2**
(config-modem 1/2)**#resource pool-member MyPool**

PRI INTERFACE COMMAND SET

To activate the PRI Interface Configuration mode, enter the **interface pri** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface pri 2
(config-pri 2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
description <text> on page 80
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

calling-party on page 2412
calling-party name-facility-timeout <value> on page 2414
connect e1<slot/port> tdm-group <number> on page 2415
connect t1 <slot/port> tdm-group <number> on page 2416
digits-transferred <value> on page 2417
isdn alert disable pi-8 on page 2418
isdn connect enable pi-2 on page 2419
isdn disconnect progress-tone on page 2420
isdn name-delivery on page 2421
isdn overlap-receive on page 2422
isdn pi-location on page 2423
isdn setup enable on page 2424
isdn supplementary-service on page 2425
isdn switch-type on page 2427
redirecting-number on page 2428
role on page 2429
snmp trap on page 2430
snmp trap link-status on page 2431

calling-party

Use the **calling-party** command to configure and control the primary rate interface (PRI) outgoing caller ID information. Use the **no** form of this command to disable this feature. Variations of this command include:

calling-party name <*name*>
calling-party number <*number*>
calling-party override always
calling-party override if-no-CID
calling-party presentation allowed
calling-party presentation not-available
calling-party presentation restricted
calling-party screening auto
calling-party screening network-provided

Syntax Description

name <*name*>	Configure the calling party name for the PRI.
number <*number*>	Configure the calling party number for the PRI.
override always	Enables the calling party to be replaced with the override number.
override if-no-CID	Enables the calling party to be replaced if caller ID no number is received.
presentation allowed	Enables the presentation of caller ID to always be allowed.
presentation not-available	Sets the calling party number to not available.
presentation restricted	Restricts the delivery on the caller ID information.
screening auto	Specifies that the calling party screening indicator is automatically determined.
screening network-provided	Specifies that the calling party screening indicator is provided by the network.

Default Values

By default, the command is disabled and the calling party screening indicator is set to **auto**.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was expanded to include the basic rate interface (PRI) and the **screening** parameters.

Usage Examples

The following example configures calling party outgoing information:

(config)**#interface pri 2**
(config-pri 2)**#calling-party override always**
(config-pri 2)**#calling-party presentation 555-8000**
(config-pri 2)**#calling-party name Company, Inc.**

calling-party name-facility-timeout <*value*>

Use the **calling-party name-facility-timeout** command to set the name facility timeout. This value determines the number of seconds to wait for the calling-party name delivery after the initial SETUP message is received. Once the name delivery is received or the timeout has passed, the corresponding INVITE is sent using the Session Initiation Protocol (SIP) trunk. Set the value to **0** to eliminate the delay. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Sets the number of seconds to wait for the calling-party name delivery. Valid range is **0** to **5**.

Default Values

By default, the timeout is **2** seconds.

Command History

Release A2.03	Command was introduced.

Usage Examples

The following example sets the **calling-party name-facility-timeout** to **5** seconds:

(config)**#interface pri 2**
(config-pri 2)**#calling-party name-facility-timeout 5**

connect e1<*slot/port*> tdm-group <*number*>

Use the **connect e1 tdm-group** command to configure the time division multiplexing (TDM) group connection used for the primary rate integrated services digital network (ISDN) primary rate interface (PRI) interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*slot/port*>	Specifies the E1 interface identifier.
<*number*>	Specifies the TDM group number. Valid range is **1** to **255**.

Default Values

By default, the command is disabled.

Command History

Release A2	Command was introduced.

Usage Examples

The following example configures the unit to connect **tdm-group 1** of the E1 to the PRI interface **2**:

(config)**#interface pri 2**
(config-pri 2)**#connect e1 0/1 tdm-group 1**

connect t1 <*slot/port*> tdm-group <*number*>

Use the **connect t1 tdm-group** command to configure the time division multiplexing (TDM) group connection used for the primary rate interface (PRI). Use the **no** form of this command to return to the default value.

Syntax Description

<*slot/port*>	Configure the T1 interface identifier.
<*number*>	Configure the TDM group number. Valid range is **1** to **255**.

Default Values

By default, the command is disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the unit to connect tdm-group 1 of the T1 to the PRI:

(config)**#interface pri 2**
(config-pri 2)**#connect t1 1/1 tdm-group 1**

digits-transferred <*value*>

Use the **digits-transferred** command to define how many of the received digits should be sent to the internal switchboard from an incoming call on a trunk. The number of digits transferred are the least digits received. Direct inward dialing (DID) should be used if a Telco provider is providing digits to the unit on inbound calls or if the unit needs to provide DID information to a piece of customer premises equipment (CPE). Use the **no** form of this command to disable this feature. Variations of this command include:

digits-transferred <*value*>
digits-transferred <*value*> **no-prefix**
digits-transferred <*value*> **prefix** <*number*>

Syntax Description

<*value*>	Specifies the number of digits to be transferred. The valid number of digits are **0**, **3**, **4**, **7** or **all**.
no-prefix	Optional. Specifies transferring the DID digits without appending a prefix.
prefix <*number*>	Optional. Specifies a sequence of digits to be appended to the digits that will be transmitted. For example, if seven digits will be transferred via DID, then prefix the seven digits with 256. Thus, **555-8000** would be prefixed with **256**, and **256-555-8000** would not.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example transfers the digits **555-8000** and adds the prefix **256**:

(config)**#interface pri 2**
(config-pri 2)**#digits-transferred 5558000 prefix 256**

isdn alert disable pi-8

Use the **isdn alert disable pi-8** command to disable progress indicator 8 in integrated services digital network (ISDN) alert messages on the primary rate interface (PRI). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, progress indicator 8 is enabled.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example disables progress indicator 8 in the alert message:

(config)**#interface pri 2**
(config-pri 2)**#isdn alert disable pi-8**

isdn connect enable pi-2

Use the **isdn connect enable pi-2** command to enable progress indicator 2 in integrated services digital network (ISDN) connect messages on the primary rate interface (PRI). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, progress indicator 2 is disabled.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example enables progress indicator 2 in the connect message:

(config)**#interface pri 2**
(config-pri 2)**#isdn connect enable pi-2**

isdn disconnect progress-tone

Use the **isdn disconnect progress-tone** command to specify that calls use a progress tone to indicate the call should be disconnected. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, call progress tones are not used.

Command History

Release R10.5.0	Command was introduced.

Usage Example

The following example enables the use of progress tones when calls are disconnected:

(config)**#interface pri 2**
(config-pri 2)**#isdn disconnect progress-tone**

isdn name-delivery

Use the **isdn name-delivery** command to control the delivery of the name associated with the primary rate interface (PRI). This command can be used to block the caller ID name on the PRI. Use the **no** form of this command to return to the default setting. Variations of this command include:

isdn name-delivery display
isdn name-delivery proceeding
isdn name-delivery setup

Syntax Description

display	Delivers the calling party's name in a display information element (IE) in the SETUP message.
proceeding	Delivers the calling party's name in a facility IE after the PROCEEDING message.
setup	Delivers the calling party's name in a facility IE in the SETUP message.

Default Values

By default, **isdn name-delivery** is disabled.

Command History

Release 11.1	Command was introduced.
Release 14.1	Command was updated.

Usage Examples

The following example configures the calling party information to be delivered in the setup message:

(config)**#interface pri 2**
(config-pri 2)**#isdn name-delivery setup**

isdn overlap-receive

Use the **isdn overlap-receive** command to enable overlap receiving mode on the primary rate interface (PRI). Use the **no** form of this command to return to the default setting. Variations of this command include:

isdn overlap-receive timeout <*value*>
isdn overlap-receive digits-transferred <*value*>

Syntax Description

timeout <*value*>	Specifies how long the interface will attempt to match direct inward dialing (DID) digits received in INFO messages to entries in the voice dial-plan. If no matching entry is found, the interface will deliver the message when the timeout period expires. Valid range is **1** to **15** seconds.
digits-transferred <*value*>	Specifies how many DID digits the interface will collect before delivering the call. Valid range is **1** to **64** digits

Default Values

By default, **isdn overlap-receive** is disabled.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

When **isdn overlap-receive** is enabled, the interface will accept a SETUP message where the Called Party Number (CPN) information element is either missing or does not have enough DID digits. When more digits are received in subsequent INFO messages, the number is matched against entries in the voice dial-plan to determine when there are enough digits to deliver the call.

If no matching voice dial-plan entry is found, the interface will deliver the call when configuration the **isdn overlap-receive timeout** expires.

When **isdn overlap-receive did-length** is configured, no voice dial-plan look-up occurs. The interface will deliver the call as soon as the specified number of DID digits has been collected.

If at any time an INFO message is received with CPN information element containing **#** or a Sending Complete information element is received, the interface will deliver the call immediately.

Usage Examples

The following example enables overlap receiving with a timeout value of **7** seconds on the PRI:

(config)**#interface PRI 2**
(config-pri 2)**#isdn overlap-receiving timeout 7**

isdn pi-location

Use the **isdn pi-location** command to configure the location of the progress indicator in integrated services digital network (ISDN) messages on the primary rate interface (PRI). The location is a progress indicator information element that indicates from where the message comes. Use the **no** form of this command to return to the default setting. Variations of this command include:

isdn pi-location private
isdn pi-location public

Syntax Description

private	Sets the location of the progress indicator to private network serving the local user.
public	Sets the location of the progress indicator to public network serving the local user.

Default Values

By default, the progress indicator location is public.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example set the progress indicator location to private:

(config)**#interface pri 2**
(config-pri 2)**#isdn pi-location private**

isdn setup enable

Use the **isdn setup enable** command to enable progress indicators in the integrated services digital network (ISDN) setup message and redirecting numbers for ISDN calls on the primary rate interface (PRI). The redirecting number is used to insert the caller's number when a call is diverted by a blind transfer or forward that both occurs on an ISDN trunk in local mode and proceeds out of an ISDN trunk. Use the **no** form of this command to disable this feature. Variations of this command include:

isdn setup enable called
isdn setup enable calling
isdn setup enable pi-1
isdn setup enable pi-3
isdn setup enable redirecting-number

Syntax Description

called	Enables the called number in ISDN setup messages.
calling	Enables the calling number in ISDN setup messages.
pi-1	Enables progress indicator 1 for ISDN setup messages. Progress indicator 1 indicates that the call is not end-to-end ISDN and further call progress information may be available in-band.
pi-3	Enables progress indicator 3 for ISDN setup messages. Progress indicator 3 indicates that the origination address is non-ISDN.
redirecting-number	Enables redirecting numbers for ISDN calls.

Default Values

By default, the called and calling numbers are included in ISDN setup messages.

Command History

Release A4.01	Command was introduced.
Release A4.03	Command was expanded to include the **redirecting-number** parameter.
Release R10.5.0	Command was expanded to include the **called** and **calling** parameters.

Usage Examples

The following example enables redirecting numbers for ISDN calls:

(config)**#interface pri 2**
(config-pri 2)**#isdn setup enable redirecting-number**

isdn supplementary-service

Use the **isdn supplementary-service** command to enable integrated services digital network (ISDN) supplementary services on a primary rate interface (PRI). Use the **no** form of this command to disable this feature. Variations of this command include:

isdn supplementary-service ect
isdn supplementary-service rlt
isdn supplementary-service tbct
isdn supplementary-service tbct active-transfers <*value*>
isdn supplementary-service tbct d-channel-id <*id number*>
isdn supplementary-service tbct d-channel-id auto
isdn supplementary-service tbct notify-controller
isdn supplementary-service tbct transfer-counters
isdn supplementary-service tbct transfer-rate <*value*>

Syntax Description

ect	Enables European Telecommunications Standards Institute (ETSI) explicit call transfer (ECT).
rlt	Enables Digital Multiplex System (DMS) release link trunk (RLT).
tbct	Enables National ISDN II two B-channel transfer (TBCT).
active-transfers <*value*>	Optional. Sets the number of simultaneous TBCT transfers. Valid range is **0** to **60000**.
d-channel-id <*id number*>	Optional. Sets the D-channel ID for TBCT on the interface.
d-channel-id auto	Optional. Sets the D-channel ID for TBCT to be automatically configured.
notify-controller	Optional. Enables TBCT notification to the controller.
transfer-counters	Optional. Enables transfer counters during TBCT.
transfer-rate <*value*>	Optional. Sets the number of transfers allowed within a 10-second interval. Valid range is **0** to **500**.

Default Values

By default, ECT, RLT, and TBCT are disabled.

By default, the **tbct active-transfers** value is set to **100**, the **tbct d-channel-id** is set to **auto**, the **tbct notify-controller** is disabled, the **tbct transfer-counters** are enabled, and the **tbct transfer-rate** is set to **10**.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example enables TBCT on PRI interface 2 and sets the number of simultaneous TBCT transfers to **5000**:

(config)**#interface pri 2**
(config-pri 2)**#isdn supplementary-service tbct**
(config-pri 2)**#isdn supplementary-service tbct active-transfers 5000**

isdn switch-type

Use the **isdn switch-type** command to configure the switch type assigned on the primary rate integrated services digital network (ISDN) primary rate interface (PRI) circuit. Telephone companies use various types of ISDN switches and this setting must match the switch type used by your provider. Use the **no** form of this command to return to the default setting. Variations of this command include:

isdn switch-type 4ess
isdn switch-type 5ess
isdn switch-type dms100
isdn switch-type etsi
isdn switch-type etsi legacy
isdn switch-type ni2

Syntax Description

4ess	Sets the ISDN switch type to ATT 4ESS.
5ess	Sets the ISDN switch type to Lucent 5ESS.
dms100	Sets the ISDN switch type to Northern ISDN II.
etsi	Sets the ISDN switch type to European Telecommunications Standards Institute (ETSI) (ETS 300 403).
etsi legacy	Sets the ISDN switch type to legacy ETSI (ETS 300 102).
ni2	Sets the ISDN switch type to National ISDN II.

Default Values

By default, the command is set to **ni2**.

Command History

Release 11.1	Command was introduced.
Release A2	Command was expanded to include the ETSI switch types.

Usage Examples

The following example configures the PRI switch type National ISDN II:

(config)**#interface pri 2**
(config-pri 2)**#isdn switch-type ni2**

redirecting-number

Use the **redirecting-number** command to configure the format in which redirecting numbers are sent on the primary rate interface (PRI). Use the **no** form of this command to return to the default setting. Variations of this command include:

redirecting-number as-received
redirecting-number prefer-national

Syntax Description

as-received	Configures the redirecting number to be sent exactly as it is received.
prefer-national	Configures the redirecting number to be sent in E.164 format, if possible.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example configures the redirecting number to be sent in E.164 format:

(config)**#interface pri 2**
(config-pri 2)**#redirecting-number prefer-national**

role

Use the **role** command to configure the interface protocol to use on the primary rate interface (PRI). This setting controls the functional mode of the interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

role network
role network b-channel-restarts disable
role network b-channel-restarts enable
role user

Syntax Description

network	Sets the port to operate in network termination (NT) mode.
b-channel-restarts disable	Optional. Disables B-channel restarts.
b-channel-restarts enable	Optional. Enables B-channel restarts.
user	Sets the port to operate in terminal equipment (TE) mode.

Default Values

By default, the role is set to **network b-channel-restarts disable**.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the interface protocol as **user** on the PRI:

(config)**#interface pri 2**
(config-pri 2)**#role user**

snmp trap

Use the snmp trap command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the no form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example enables SNMP on the primary rate interface (PRI) 2:

(config)**#interface pri 2**
(config-pri 2)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release A5.01	Command was introduced.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the primary rate interface (PRI) 2:

(config)**#interface pri 2**
(config-pri 2)**#no snmp trap link-status**

SERIAL INTERFACE COMMAND SET

To activate the Serial Interface Configuration mode, enter the **interface serial** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface serial 1/1
(config-ser 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

et-clock-source on page 2433
ignore dcd on page 2434
invert etclock on page 2435
invert rxclock on page 2436
invert txclock on page 2437
serial-mode on page 2438
snmp trap on page 2439
snmp trap link-status on page 2440

et-clock-source

Use the **et-clock-source** command to configure the clock source used when creating the external transmit reference clock (et-clock). Use the **no** form of this command to return to the default value. Variations of this command include:

et-clock-source rxclock
et-clock-source txclock

Syntax Description

rxclock	Uses the clock recovered from the receive signal to generate et-clock.
txclock	Uses the clock recovered from the transmit signal to generate et-clock.

Default Values

By default, the clock recovered from the transmit signal is used to generate the et-clock.

Command History

Release 1.1	Command was introduced.

Functional Notes

The external transmit clock (et-clock) is an interface timing signal (provided by the data terminal equipment (DTE) device) used to synchronize the transfer of transmit data.

Usage Examples

The following example configures the serial interface to recover the clock signal from the received signal and use it to generate et-clock:

(config)**#interface serial 1/1**
(config-ser 1/1)**#et-clock-source rxclock**

ignore dcd

Use the **ignore dcd** command to specify the behavior of the serial interface when the data carrier detect (DCD) signal is lost. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, the serial interface does not ignore a change in status of the DCD signal.

Command History

Release 1.1	Command was introduced.

Functional Notes

When configured to follow DCD (default condition), the serial interface will not attempt to establish a connection when DCD is not present. When configured to ignore DCD, the serial interface will continue to attempt to establish a connection even when DCD is not present.

Usage Examples

The following example configures the serial interface to ignore a loss of the DCD signal:

(config)**#interface serial 1/1**
(config-ser 1/1)**#ignore dcd**

invert etclock

Use the **invert etclock** command to configure the serial interface to invert the external transmit reference clock (et-clock) in the data stream before transmitting. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, the serial interface does not invert et-clock.

Command History

Release 1.1	Command was introduced.

Functional Notes

If the serial interface cable is long, causing a phase shift in the data, the et-clock can be inverted using the **invert etclock** command. This switches the phase of the clock, which compensates for a long cable.

Usage Examples

The following example configures the serial interface to invert et-clock:

(config)**#interface serial 1/1**
(config-ser 1/1)**#invert etclock**

invert rxclock

Use the **invert rxclock** command to configure the serial interface to expect an inverted receive clock (found in the received data stream). Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, the serial interface does not expect an inverted receive clock (**rxclock**).

Command History

Release 1.1	Command was introduced.

Functional Notes

If the serial interface cable is long, causing a phase shift in the data, the transmit clock can be inverted using the **invert txclock** command (refer to *invert txclock on page 2437*). This switches the phase of the clock, which compensates for a long cable. If the transmit clock of the connected device is inverted, use the **invert rxclock** command to configure the receiving interface appropriately.

Usage Examples

The following example configures the serial interface to invert receive clock:

(config)**#interface serial 1/1**
(config-ser 1/1)**#invert rxclock**

invert txclock

Use the **invert txclock** command to configure the serial interface to invert the transmit clock (found in the transmitted data stream) before sending the signal. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, the serial interface does not invert transmit clock (**txclock)**.

Command History

Release 1.1	Command was introduced.

Functional Notes

If the serial interface cable is long, causing a phase shift in the data, the transmit clock can be inverted (using the **invert txclock** command). This switches the phase of the clock, which compensates for a long cable. If the transmit clock of the connected device is inverted, use the **invert rxclock** command to configure the receiving interface appropriately.

Usage Examples

The following example configures the serial interface to invert the transmit clock:

(config)**#interface serial 1/1**
(config-ser 1/1)**#invert txclock**

serial-mode

Use the **serial-mode** command to specify the electrical mode for the interface. Use the **no** form of this command to return to the default value. Variations of this command include:

serial-mode eia530
serial-mode v35
serial-mode x21

Syntax Description

eia530	Configures the interface for use with the EIA 530 adapter cable (P/N 1200883L1).
v35	Configures the interface for use with the V.35 adapter cable (P/N 1200873L1).
x21	Configures the interface for use with the X.21 adapter cable (P/N 1200874L1).

Default Values

By default, the serial interface is configured for a **V.35** adapter cable.

Command History

Release 1.1	Command was introduced.

Functional Notes

The pinouts for each of the available interfaces can be found in the *Hardware configuration guide* located online at http://supportforums.adtran.com.

Usage Examples

The following example configures the serial interface to work with the **X.21** adapter cable:

(config)**#interface serial 1/1**
(config-ser 1/1)**#serial-mode x21**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP on the serial interface:

(config)**#interface serial 1/1**
(config-ser 1/1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the serial interface:

(config)**#interface serial 1/1**
(config-ser 1/1)**#no snmp trap link-status**

SHDSL INTERFACE COMMAND SET

To activate the Single-Pair High-Speed Digital Subscriber Line (SHDSL) Interface Configuration mode, enter the **interface shdsl** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface shdsl 1/1
(config-shdsl 1/1)#
```

*Not all SHDSL commands apply to all SHDSL interfaces. Type **interface shdsl <slot/port>** to display a list of valid commands.*

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

alarm-threshold on page 2443
annex on page 2444
boot alternate-image on page 2445
equipment-type on page 2446
ignore-error-duration <time> on page 2447
inband-detection on page 2448
inband-protocol on page 2449
line-mode on page 2450
linerate <value> on page 2451
linerate adaptive <min DS0s-max DS0s> <target dBs> on page 2452
linerate fixed <min DS0s-max DS0s> on page 2453
loopback on page 2454
loopback remote inband on page 2455
outage-retrain on page 2456

alarm-threshold

Use the **alarm-threshold** command to set thresholds for specific alarm conditions. Use the **no** form of this command to disable threshold settings. Variations of this command include:

alarm-threshold loop-attenuation <*value*>
alarm-threshold snr-margin <*value*>

Syntax Description

loop-attenuation <*value*>	Specifies a loop-attenuation threshold value from 1 to 127 dB. If signal energy loss on the loop exceeds the configured value, the router issues an alarm.
snr-margin <*value*>	Specifies a value for signal-to-noise ratio (SNR) margin from 1 to 15 dB. If the difference in amplitude between the baseband signal and the noise exceeds the configured value, the router issues an alarm.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example sets the loop attenuation threshold at **45** dB:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#alarm-threshold loop-attenuation 45**

annex

Use the **annex** command to select the single-pair, high-speed digital subscriber line (SHDSL) operating mode supported on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

annex a
annex a-efm
annex a-or-b
annex a-or-b-efm
annex b
annex b-efm
annex b
annex efm

Syntax Description

a	Specifies Annex A (North American operating parameters).
a-efm	Specifies Annex A and IEEE 802.3ah handshake parameters.
a-or-b	Specifies Annex A or Annex B. This parameter enables the detection and selection of the annex type depending on the connected terminating unit.
a-or-b-efm	Specifies Annex A or Annex B and IEEE 802.3ah handshake parameters. This parameter enables the detection and selection of the annex type depending on the connected terminating unit.
b	Specifies Annex B (European operating parameters).
b-efm	Specifies Annex B and IEEE 802.3ah handshake parameters.
efm	Specifies IEEE 802.3ah handshake parameters.

Default Values

By default, the SHDSL operating mode is set to **a-or-b**.

Command History

Release 15.1	Command was introduced.
Release R10.6.0	Command was expanded to include the **a-efm**, **a-or-b-efm**, **b-efm**, and **efm** parameters.

Usage Examples

The following example sets the operating mode to **annex a**:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#annex a**

boot alternate-image

Use the **boot alternate-image** command to execute new code after a firmware upgrade.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.

Functional Notes

The current single-pair high-speed digital subscriber line (SHDSL) network interface module (NIM) card (P/N 1200867L1) supports two code images commonly referred to as the active image and the inactive image. When a firmware upgrade is performed on the card (through the **copy** <*filename*> **interface shdsl x/y** Enable mode command), the new firmware is placed in the inactive image space. This new code will not be executed until the **boot alternate-image** command is issued. When the user does this, the NIM will reboot (taking the current line down) with the new code. At this point, the old code becomes the inactive image and the new recently updated code becomes the active image.

Usage Examples

The following example causes the firmware upgrade to take effect:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#boot alternate-image**

equipment-type

Use the **equipment-type** command to determine the operating mode for the single-pair high-speed digital subscriber line (SHDSL) interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

equipment-type co
equipment-type cpe

Syntax Description

co	Use this option only in a campus environment when operating two SHDSL network interface modules (NIMs) back-to-back. In this setup, configure the master NIM to CO and the slave NIM to customer premises equipment (CPE).
cpe	Use this option when interfacing directly with your service provider or when acting as the slave NIM in a campus environment.

Default Values

The default for this command is **cpe**.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example changes the operating mode of the SHDSL interface to CO:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#equipment-type co**

ignore-error-duration <*time*>

Use the **ignore-error-duration** command to specify the amount of time that errors are ignored during line training. Use the **no** form of this command to return to the default setting.

Syntax Description

<*time*>	Specifies time in seconds. Valid range is **15** to **30** seconds.

Default Values

By default, **ignore-error-duration** is set to **15** seconds.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets the amount of time errors are ignored during line training to **25** seconds:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#ignore-error-duration 25**

inband-detection

Use the **inband-detection** command to enable inband loopback pattern detection on the single-pair high-speed digital subscriber line (SHDSL) interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example disables inband loopback pattern detection:

```
(config)#interface shdsl 1/1
(config-shdsl 1/1)#no inband-detection
```

inband-protocol

Use the **inband-protocol** command to designate the inband loopback pattern to send/detect on the single-pair high-speed digital subscriber line (SHDSL) interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

inband-protocol pn127
inband-protocol v54

Syntax Description

pn127	Selects PN127 as the inband loopback pattern to send/detect.
v54	Selects V.54 as the inband loopback pattern to send/detect.

Default Values

By default, the inband loopback pattern is set to **v54**.

Command History

Release 4.1	Command was introduced.

Functional Notes

Inband loopbacks are specific patterns that are sent in place of user data to trigger a loopback. Both PN127 and V.54 are industry standard loopback patterns used to allow remote loopbacks.

Usage Examples

The following example sets the inband loopback pattern for **pn127**:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#inband-protocol pn127**

line-mode

Use the **line-mode** command to select the controller line mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

line-mode 2-wire
line-mode 4-wire

Syntax Description

2-wire	Specifies two-wire mode.
4-wire	Specifies four-wire mode for extended operation.

Default Values

By default, the digital subscriber line (DSL) operating mode is set to **2-wire**.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets the line mode to **4-wire**:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#line-mode 4-wire**

linerate *<value>*

Use the **linerate** command to define the line rate for the single-pair high-speed digital subscriber line (SHDSL) interface (the value includes 8 kbps of framing overhead). This command is functional only in CO operating mode (refer to *equipment-type on page 2446*). The first two selections listed in the command line interface (CLI) (72 and 136 kbps) are not supported by the SHDSL network interface module (NIM) (P/N 1200867L1). Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the line rate in kbps. Range is **200** to **2312** kbps in 64k increments.

Default Values

By default, the line rate is set to **2056** kbps.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example changes the line rate of the SHDSL interface to **264** kbps:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#linerate 264**

linerate adaptive *<min DS0s-max DS0s> <target dBs>*

Use the **linerate adaptive** command to configure the single-pair, high-speed digital subscriber line (SHDSL) interface for adaptive line rate training according to the signal quality conditions on the line. Variations of this command include:

linerate adaptive <*min DS0s-max DS0s*> <*target dBs*> **current-condition**
linerate adaptive <*min DS0s-max DS0s*> <*target dBs*> **worstcase-condition**

Syntax Description

<min DS0s-max DS0s>	Specifies a range of DS0s for the minimum and maximum possible values for the linerate in the format <minimum number of DS0s-maximum number of DS0s>. The line rate is determined by multiplying the DS0 number by 64 kbps. The default range is **3-89** DS0s.
<target dBs>	Specifies the target signal quality margin desired for the interface. Valid range is **-10** to **20** dBs. The default value is **3** dBs.
current-condition	Configures the SHDSL interface for adaptive line rate training according to current signal quality conditions on the line. This mode is not recommended per ITU-T G991.2 Section 6.3.6.
worstcase-condition	Configures the SHDSL interface for adaptive line rate training according to worst-case signal quality conditions on the line.

Default Values

The default value for this command is **linerate adaptive 3-89 3 worstcase-condition**.

Command History

Release R10.6.0	Command was introduced.

Usage Examples

The following example configures the SHDSL interface for adaptive line rate training according to worst-case signal quality conditions on the line.

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#linerate adaptive 3-64 5 worstcase-condition**

linerate fixed *<min DS0s-max DS0s>*

Use the **linerate fixed** command to configure the single-pair, high-speed digital subscriber line (SHDSL) interface for fixed adaptive line rate training. When in this mode, no line probing is performed by the interface. The line rate is determined by comparing the range of level zero digital signals (DS0s) specified with what is allowed by the other end point during the SHDSL handshake process.

Syntax Description

<min DS0s-max DS0s>	Specifies a range of DS0s for the minimum and maximum possible values for the linerate in the format <minimum number of DS0s-maximum number of DS0s>. The line rate is determined by multiplying the DS0 number by 64 kbps. The default range is **3-89** DS0s.

Default Values

No default values are necessary for this command.

Command History

Release R10.6.0	Command was introduced.

Usage Examples

The following example configures the SHDSL interface for fixed line rate training:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#linerate fixed 3-64**

loopback

Use the **loopback** command to initiate a loopback test on the single-pair high-speed digital subscriber line (SHDSL) interface. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback analog
loopback digital
loopback network
loopback remote

Syntax Description

analog	Loops the circuit at the analog hybrid.
digital	Loops the circuit at the framer.
network	Loops data back towards the network.
remote	Transmits a network loopback request. This command is functional only in CO operating mode (refer to *equipment-type on page 2446*).

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 15.1	Command was expanded to include the analog and digital loopbacks.

Usage Examples

The following example initiates a loopback test on the SHDSL interface that will loop the data back toward the network:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#loopback network**

loopback remote inband

Use the **loopback remote inband** command to inject the selected inband loop-up pattern into the data stream to cause a loopback at the far end. Use the **no** form of this command to inject a loop-down pattern into the data stream to cause an existing inband loopback at the far end to cease.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example injects a loop-down pattern into the data stream, causing existing loopbacks at the far end to stop:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#no loopback remote inband**

outage-retrain

Use the **outage-retrain** command to cause the single-pair high-speed digital subscriber line (SHDSL) interface to force the SHDSL retrain sequence (which takes the line down temporarily) if the interface detects more than ten consecutive errored seconds. A retrain is forced in hopes that the newly retrained line will achieve better performance than the previous training state. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example forces a retrain sequence on the SHDSL interface:

```
(config)#interface shdsl 1/1
(config-shdsl 1/1)#outage-retrain
```


snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Us the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Usage Examples

The following example enables SNMP capability on the SHDSL interface:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the SHDSL interface:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#no snmp trap link-status**

test-pattern

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the selected test pattern toward the network. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation. Variations of this command include:

test-pattern clear
test-pattern errors
test-pattern insert
test-pattern p215

Syntax Description

clear	Clears the test pattern error count.
errors	Displays the test pattern error count.
insert	Inserts an error into the currently active test pattern.
p215	Generates a pseudorandom test pattern sequence based on a 15-bit shift register.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example sends a **p215** test pattern:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#test-pattern p215**

test splice-detect distance-type

Use the **test splice-detect distance-type** command to specify the unit of measurement used in the bad splice detection test. Use the **no** form of this command to return to the default unit of measurement. Variations of this command include:

test splice-detect distance-type feet
test splice-detect distance-type meters

Syntax Description

feet	Specifies the distance to the detected bad splice is measured in feet.
meters	Specifies the distance to the detected bad splice is measured in meters.

Default Values

By default, distances in the bad splice detection test are measured in feet.

Command History

Release A4.05	Command was introduced.

Functional Notes

The bad splice detection test is a line testing feature that allows users to locate intermittent faults in lines by estimating the distance to the fault. Splice detection is always enabled on the SHDSL EFM NIM2 module and it continually monitors the signal-to-noise ratio (SNR) of the connection. When a negative change in the SNR is detected, a measurement is taken to determine the distance to where the issue is possibly occurring on the line. Bad splice detection test results can be viewed using the command *show interfaces shdsl <slot/port> splice-detect on page 691*.

Usage Examples

In the following example, the unit of measurement used by the bad splice detection test is changed from feet to meters:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#test splice-detect distance-type meters**

test tscan

Use the **test tscan** command to initiate a Tscan test, as well as configure and display Tscan test parameters for the interface. Variations of this command include:

test tscan
test tscan clear-results
test tscan display-results

Syntax Description

clear-results	Clears the Tscan test results from previously completed Tscan tests.
display-results	Displays the results of the most recently completed Tscan test.

Default Values

By default, Tscan tests are not run on the interface.

Command History

Release A4.05	Command was introduced.

Functional Notes

The Tscan line test is a testing feature that allows users to isolate faults in lines by estimating the distance to the fault and determining the type of fault, whether a short or an open connection. Tscan is an intrusive test, which causes trained SHDSL loops to go down, but it is useful as a method for finding faults in loops that will not train, rather than as a performance metric for operational loops.

Tscan tests can be started on any port that is enabled. Tscan tests typically take from 20 seconds to one minute to complete, and timeout after 90 seconds to restore control to the command line interface (CLI). When the test is complete, results are displayed in the CLI or can be viewed at a later time using the command **test tscan display-results**. Displayed results include the date and time of the test, the status of the test, the line rate used while Tscan operates (typically 16 or 32 DSOs), the distance to the fault if one is detected (displayed in feet), and the fault type that is found. The minimum distance for the Tscan test is **0** feet and the maximum Tscan test distance is **1200** feet.

Usage Examples

The following example initiates a Tscan test on SHDSL interface **1/1**:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#test tscan**

The following example displays results from a recently completed Tscan test:

(config)**#interface shdsl 1/1**
(config-shdsl 1/1)**#test tscan display-results**
shdsl 1/1 TSCAN Results
Date/Time: Thu, October 28, 2010 04:30:59 PM, CDT
Status: Done
Rate: 32 DSOs
Distance: 1100 ft
Fault: Open

T1 INTERFACE COMMAND SET

To activate the T1 Interface Configuration mode, enter the **interface t1** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface t1 1/1
(config-t1 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

All other commands for this command set are described in this section in alphabetical order.

clock source

Use the **clock source** command to configure the source timing used for the interface. Use the **no** form of this command to return to the default value. Variations of this command include:

clock source internal
clock source line
clock source system
clock source through
clock source through t1 *<interface id>*

Syntax Description

internal	Configures the unit to provide clocking using the internal oscillator.
line	Configures the unit to recover clocking from the T1 circuit.
system	Configures the unit to provide clocking using the system clock.
through	Configures the unit to recover clocking from the circuit connected to the DSX-1 interface.
through t1 *<interface id>*	Configures the unit to recover clocking from the alternate interface. Only valid on T1 systems with multiple T1 interfaces and a single clock source.

Default Values

By default, the **clock source** is set to **line**.

Command History

Release 1.1	Command was introduced.
Release 13.1	Command was expanded to include the system as a clocking source.

Functional Notes

When operating on a circuit that is providing timing, setting the **clock source** to **line** can avoid errors, such as clock slip seconds (CSS).

Usage Examples

The following example configures the unit to recover clocking from the primary circuit:

(config)**#interface t1 1/1**
(config-t1 1/1)**#clock source line**

coding

Use the **coding** command to configure the line coding for a T1 physical interface. This setting must match the line coding supplied on the circuit by the service provider. Use the **no** form of this command to return to the default setting. Variations of this command include:

coding ami
coding b8zs

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
b8zs	Configures the line coding for bipolar eight zero substitution (B8ZS).

Default Values

By default, all T1 interfaces are configured with **b8zs** line coding.

Command History

Release 1.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the T1 circuit. A mismatch will result in line errors (e.g., bipolar violations (BPVs)).

Usage Examples

The following example configures the T1 interface for **ami** line coding:

(config)**#interface t1 1/1**
(config-t1 1/1)**#coding ami**

fdl

Use the **fdl** command to configure the format for the facility data link (FDL) channel on the T1 circuit. FDL channels are only available on point-to-point circuits. Use the **no** form of this command to return to the default value. Variations of this command include:

fdl ansi
fdl att
fdl none

Syntax Description

ansi	Configures the FDL for ANSI T1.403 standard.
att	Configures the FDL for AT&T TR 54016 standard.
none	Disables FDL on this circuit.

Default Values

By default, the FDL is configured for **ansi**.

Command History

Release 1.1	Command was introduced.

Functional Notes

T1 circuits using extended superframe (ESF) framing format (specified using the **framing** command) reserve 12 bits as a data link communication channel, referred to as the FDL, between the equipment on either end of the circuit. The FDL allows the transmission of trouble flags, such as the Yellow Alarm signal. Refer to *framing on page 2467* for related information.

Usage Examples

The following example disables the FDL channel for the T1 circuit:

(config)**#interface t1 1/1**
(config-t1 1/1)**#fdl none**

framing

Use the **framing** command to configure the framing format for the T1 interface. This parameter should match the framing format supplied by your network provider. Use the **no** form of this command to return to the default value. Variations of this command include:

framing d4
framing esf

Syntax Description

d4	Specifies D4 superframe (SF) format.
esf	Specifies extended superframe (ESF) format.

Default Values

By default, the framing format is set to **esf**.

Command History

Release 1.1	Command was introduced.

Functional Notes

A frame is comprised of a single byte from each of the T1's timeslots; there are 24 timeslots on a single T1 circuit. Framing bits are used to separate the frames and indicate the order of information arriving at the receiving equipment. D4 and ESF are two methods of collecting and organizing frames over the circuit.

Usage Examples

The following example configures the T1 interface for D4 framing:

(config)**#interface t1 1/1**
(config-t1 1/1)**#framing d4**

lbo

Use the **lbo** command to configure the line build out (LBO) for the T1 interface. Use the **no** form of this command to return to the default value. Variations of this command include:

lbo short <*value*>
lbo long <*value*>

Syntax Description

long <*value*>	Configures the LBO (in dB) for T1 interfaces with cable lengths greater than 655 feet. Choose from **-22.5**, **-15**, **-7.5**, and **0** dB.
short <*value*>	Configures the LBO (in feet) for T1 interfaces with cable lengths less than 655 feet. Range is **0** to **655** feet.

Default Values

By default, the build out is set to **0** dB.

Command History

Release 1.1	Command was introduced.

Functional Notes

LBO is artificial attenuation of a T1 output signal to simulate a degraded signal. This is useful to avoid overdriving a receiver's circuits. The shorter the distance between T1 equipment (measured in cable length), the greater the attenuation value. For example, two units in close proximity should be configured for the maximum attenuation (-22.5 dB).

Usage Examples

The following example configures the T1 interface LBO for **-22.5** dB:

(config)**#interface t1 1/1**
(config-t1 1/1)**#lbo -22.5**

loopback network

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback network line
loopback network payload

Syntax Description

line	Initiates a metallic loopback of the physical T1 network interface.
payload	Initiates a loopback of the T1 framer (CSU portion) of the T1 network interface.

Default Values

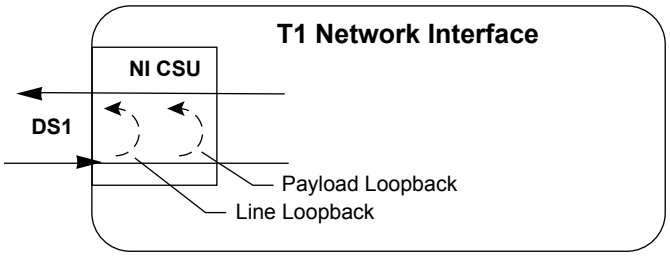
No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a payload loopback of the T1 interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#loopback network payload**

loopback remote line

Use the **loopback remote line** command to send a loopback code to the remote unit to initiate a line loopback. Use the **no** form of this command to send a loopdown code to the remote unit to deactivate the loopback. Variations of this command include:

loopback remote line fdl
loopback remote line inband

Syntax Description

fdl	Uses the facility data link (FDL) to initiate a full 1.544 Mbps physical (metallic) loopback of the signal received by the remote unit from the network.
inband	Uses the inband channel to initiate a full 1.544 Mbps physical (metallic) loopback of the signal received by the remote unit from the network.

Default Values

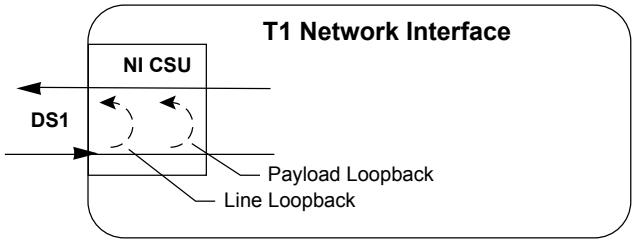
No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a remote line loopback using the FDL:

(config)**#interface t1 1/1**
(config-t1 1/1)**#loopback remote line fdl**

loopback remote payload

Use the **loopback remote payload** command to send a loopback code to the remote unit to initiate a payload loopback. A payload loopback is a 1.536 Mbps loopback of the payload data received from the network maintaining bit-sequence integrity for the information bits by synchronizing (regenerating) the timing. Use the **no** form of this command to send a loopdown code to the remote unit to deactivate the loopback.

Syntax Description

No subcommands.

Default Values

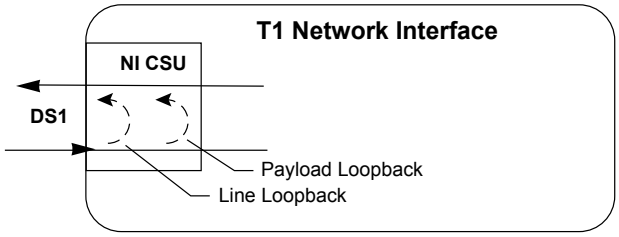
No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a remote payload loopback:

(config)**#interface t1 1/1**
(config-t1 1/1)**#loopback remote payload**

remote-alarm rai

The **remote-alarm rai** command selects the alarm signaling type to be sent when a loss of frame is detected on the T1 receive signal. Use the **no** form of this command to disable all transmitted alarms.

Syntax Description

rai	Specifies sending a remote alarm indication (RAI) in response to a loss of frame. Also, prevents a received RAI from causing a change in interface operational status.

Default Values

The default for this command is **rai**.

Command History

Release 7.1	Command was expanded to include the T1 interface.

Usage Examples

The following example enables transmission of RAI in response to a loss of frame:

(config)**#interface t1 1/1**
(config-t1 1/1)**#remote-alarm rai**

remote-loopback

Use the **remote-loopback** command to configure the interface to respond to loopbacks initiated by a remote unit (or the service provider). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables remote loopbacks on the T1 interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#remote-loopback**

snmp trap line-status

Use the **snmp trap line-status** command to control the Simple Network Management Protocol (SNMP) variable dsx1LineStatusChangeTrapEnable (RFC 2495) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the dsx1LineStatusChangeTrapEnable object identifier (OID) is set to enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 11.1	Command was introduced.

Functional Notes

The **snmp trap line-status** command is used to control the RFC 2495 dsx1LineStatusChangeTrapEnable OID (OID number 1.3.6.1.2.1.10.18.6.1.17.0).

Usage Examples

The following example disables the line-status trap on the T1 interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#no snmp trap line-status**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the T1 interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#no snmp trap link-status**

snmp trap threshold-reached

Use the **snmp trap threshold-reached** command to control the Simple Network Management Protocol (SNMP) variable adGenAOSDs1ThresholdReached (adGenAOSDs1-Ext MIB) to enable the interface to send SNMP traps when a DS1 performance counter threshold is reached. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the adGenAOSDs1ThresholdReached object identifier (OID) is disabled for all interfaces.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example disables SNMP threshold reached trap on the T1 interface:

(config)**#interface t1 1/1**
(config-t1 1/1)**#no snmp trap threshold-reached**

system-timing

Use the **system-timing** command to configure the Rx clock as the primary or secondary timing source for the system. Use the **no** form of this command to disable this feature.Variations of this command include:

system-timing primary
system-timing secondary

Syntax Description

primary	Specifies the Rx clock as the primary timing source.
secondary	Specifies the Rx clock as the secondary timing source.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example configures the T1 interface to provide its Rx clock as the primary timing source for the system:

(config)**#interface t1 1/1**
(config-t1 1/1)**#system timing primary**

tdm-group <*number*>

Use the **tdm-group** command to create a group of contiguous level zero digital signals (DS0s) on this interface to be used during the **cross-connect** process. Refer to *cross-connect on page 76* for related information. Use the **no** form of this command to remove configured time division multiplexing (TDM) groups. Variations of this command include:

tdm-group <*number*> **timeslots** <*value*>
tdm-group <*number*> **timeslots** <*value*> **speed [56 | 64]**

*Changing **tdm-group** settings could result in service interruption.*

Syntax Description

<*number*>	Identifies the created TDM group. Valid range is **1** to **255**.
timeslots <*value*>	Specifies the channels to be used in the TDM group. Valid range is **1** to **31**. The timeslot value can be entered as a single number representing one of the 31 E1 channel timeslots or as a contiguous group of channels. (For example, **1-10** specifies the first 10 channels of the E1.)
speed [56 | 64]	Optional. Specifies the individual DS0 rate on the T1 interface to be 64 kbps. Only the T1 + DSX-1 network interface module (NIM) supports the 56 kbps DS0 rate. The default speed is 64 kbps.

Default Values

By default, there are no configured TDM groups.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example creates a TDM group (labeled **5**) of 10 DS0s at 64 kbps each:

(config)**#interface t1 1/1**
(config-t1 1/1)**#tdm-group 5 timeslots 1-10 speed 64**

test-pattern

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation. Variations of this command include:

test-pattern clear
test-pattern errors
test-pattern insert
test-pattern ones
test-pattern p215
test-pattern p220
test-pattern p511
test-pattern qrss
test-pattern zeros

Syntax Description

clear	Clears the test pattern error count.
errors	Displays the test pattern errored seconds.
insert	Inserts an error into the currently active test pattern.
ones	Generates a test pattern of continuous ones.
p215	Generates a pseudorandom test pattern sequence based on a 15-bit shift register.
p220	Generates a pseudorandom test pattern sequence based on a 20-bit shift register.
p511	Generates a test pattern of repeating ones and zeros.
qrss	Generates a test pattern of random ones and zeros.
zeros	Generates a test pattern of continuous zeros.

Default Values

No default values are necessary for this command.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example activates the pattern generator for a stream of continuous **ones**:

(config)**#interface t1 1/1**
(config-t1 1/1)**#test-pattern ones**

timing-domain <*domain*>

Use the **timing-domain** command to assign the interface to a system-wide voice timing domain. Use the **no** form of this command to return to the default.

Syntax Description

<*domain*>	Assigns the interface to a system-wide timing domain. Valid domains are **1** and **2**.

Default Values

By default, interfaces are assigned to timing domain **1**.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example assigns the interface to timing domain **2**:

(config)**#interface t1 1/1**
(config-t1 1/1)**#timing-domain 2**

T3 INTERFACE COMMAND SET

To activate the T3 Interface Configuration mode, enter the **interface t3** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface t3 1/1
(config-t3 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

All other commands for this command set are described in this section in alphabetical order.

clock source

Use the **clock source** command to configure the source timing used for the interface. The clock specified using the **clock source** command is also the system master clock. Use the **no** form of this command to return to the default value. Variations of this command include:

clock source local
clock source loop

Syntax Description

local	Configures the unit to provide clocking using the internal oscillator.
loop	Configures the unit to recover clocking from the T3 circuit.

Default Values

By default, all T3 interfaces are configured with **loop** as the clock source.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example configures the unit to recover clocking from the circuit:

(config)**#interface t3 1/1**
(config-t3 1/1)**#clock source loop**

coding b3zs

Use the **coding b3zs** command to configure the line coding for a T3 physical interface. This setting must match the line coding supplied on the circuit by the service provider.

Syntax Description

b3zs	Configures the line coding for bipolar three zero substitution (B3ZS).

Default Values

By default, all T3 interfaces are configured with **b3zs** line coding.

Command History

Release 6.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the T3 circuit. A mismatch will result in line errors (e.g., bipolar violations (BPVs)).

Usage Examples

The following example configures the T1 interface for **b3zs** line coding:

(config)**#interface t3 1/1**
(config-t3 1/1)**#coding b3zs**

framing

Use the **framing** command to configure the network framing format for a T3 physical interface. Use the **no** form of this command to return to the default value. Variations of this command include:

framing cbit
framing m13

Syntax Description

cbit	Configures the interface for C-bit parity framing.
m13	Configures the interface for M13 framing.

Default Values

By default, all T3 interfaces are configured for **cbit** parity framing.

Command History

Release 6.1	Command was introduced.

Functional Notes

M13 is an asynchronous framing format that uses all 21 DS3 M-Frame C-bits for bit stuffing indicators. End-to-end path parity and datalink capabilities are not provided by the standard M13 format. C-bit parity framing differs from M13 by allowing monitoring of the data path (end-to-end) and supporting out-of-band (OOB) data links.

Usage Examples

The following example configures the T3 interface for **m13** framing:

(config)**#interface t3 1/1**
(config-t3 1/1)**#framing m13**

line-length

Use the **line-length** command to configure the line length for a T3 physical interface. Use the **no** form of this command to return to the default value. Variations of this command include:

line-length long
line-length short

Syntax Description

long	Configures the line length for a distance of 225 to 450 feet of cable.
short	Configures the line length for a distance of 0 to 225 feet of cable.

Default Values

By default, all T3 interfaces are configured for a **short** line length.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example configures the T3 interface for **long** line length:

(config)**#interface t3 1/1**
(config-t3 1/1)**#line-length long**

loopback network

Use the **loopback network** command to initiate a local T3 loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback network line
loopback network payload

Syntax Description

line	Initiates a loopback of the physical T3 network interface; that is, data received on the T3 is transmitted back out on the T3.
payload	Initiates a loopback of the T3 framer (TSU portion) of the T3 network interface.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example initiates a payload loopback of the T3 interface:

(config)**#interface t3 1/1**
(config-t3 1/1)**#loopback network payload**

loopback remote

Use the **loopback remote** command to initiate a loopback test on the T3 interface that sends a remote loopback code out the T3 circuit to loop up the far end. This command only applies when C-bit framing is used on the circuit. Use the **no** form of this command to deactivate the loopback. Variations of this command include:

loopback remote line
loopback remote payload

Syntax Description

line	Initiates a line loopback.
payload	Initiates a payload loopback.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Usage Examples

This example initiates a remote loopback on the T3 interface:

(config)**#interface t3 1/1**
(config-t3 1/1)**#loopback remote**

remote-loopback

Use the **remote-loopback** command to configure the T3 interface to be looped *from* the far end (remote device, Telco, etc.). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Command History

Release 6.1	Command was introduced.

Usage Examples

This example enables remote loopbacks on the T3 interface:

(config)**#interface t3 1/1**
(config-t3 1/1)**#remote-loopback**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high link data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example disables the link-status trap on the T3 interface:

(config)**#interface t3 1/1**
(config-t3 1/1)**#no snmp trap link-status**

test-pattern

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the selected test pattern toward the network. This pattern generation can verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation. Variations of this command include:

test-pattern clear
test-pattern errors
test-pattern insert
test-pattern ones
test-pattern p215
test-pattern p223
test-pattern zeros

Syntax Description

clear	Clears the test pattern error count.
errors	Displays the test pattern error count.
insert	Inserts an error into the currently active test pattern.
ones	Generates a test pattern of continuous ones.
p215	Generates a pseudorandom test pattern sequence based on a 15-bit shift register.
p223	Generates a pseudorandom test pattern sequence based on a 23-bit shift register.
zeros	Generates a test pattern of continuous zeros.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example enables a **p215** test pattern:

(config)**#interface t3 1/1**
(config-t3 1/1)**#test-pattern p215**

T4 INTERFACE COMMAND SET

The T4 interface is used to supply configurable synchronous clock output for network synchronization (Network Sync). You can configure the output format and output squelch threshold for the interface. Enter the T4 interface configuration mode by entering the **interface** <*interface*> command from the Global Configuration mode as follows:

```
(config)#interface t4 0/1
(config-t4 0/1)#
```

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

alias "<text>" on page 75
do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

format on page 2492
minimum-ssm-ql <value> on page 2493

format

Use the **format** command to specify the output format for the clock. Use the **no** form of this command to return to the default output format. Variations of this command include:

format ds1 d4
format ds1 esf
format e12 cas
format e12 ccs
format t12

Syntax Description

ds1 ds4	Specifies a 1544 kbps synchronization interface (DS1-D4/DS1-SF).
ds1 esf	Specifies a 1544 kbps synchronization interface with extended superframing (DS1-ESF).
e12 cas	Specifies a 2048 kbps synchronization interface (E12) with channel associated signaling pulse code modulation 30 (CAS PCM30) framing.
e12 ccs	Specifies a 2048 kbps synchronization interface (E12) with common channel signaling pulse code modulation 31 (CCS PCM31) framing.
t12	Specifies a 2048 kHz synchronization interface (T12).

Default Values

By default, the format is set to **t12**.

Command History

Release R10.11.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **e12 cas** and **e12 ccs** parameters, and the hyphen was removed from the **ds1** parameters.

Usage Examples

The following example changes the clock output format to **e12**:

(config)**#interface t4 0/1**
(config-t4 0/1)**#format e12**

minimum-ssm-ql <*value*>

Use the **minimum-ssm-ql** command to specify a squelch level for the T4 interface output. When the quality level (QL) of the synchronization status message (SSM) received by the Network Ethernet synchronization message channel (ESMC) process is below this level, the output is squelched. Use the **no** form of this command to disable this feature, which results in the output never being squelched.

Syntax Description

<*value*>	Specifies the minimum level of the synchronization status message (SSM) for the output to be active. Refer to the **Functional Notes** of this command for specific details.

Default Values

By default, squelch is disabled. The output is always active.

Command History

Release R10.11.0	Command was introduced.
Release R11.7.0	Command was altered to remove the following parameters: **ql-dnu** for EEC Option 1 and **ql-dus**, **ql-prov**, and **ql-smc** for EEC Option 2.

Functional Notes

The various <*value*> parameters available for SSM override vary according to the Ethernet equipment clock (EEC) option selected in the network synchronization (Network Sync) configuration (refer to the command *eec-option on page 4437*). If you have not specified an EEC option, Option 2 is used by default. The following lists outline the <*value*> parameters for the **minimum-ssm-ql** command.

SSM Override Parameters for EEC Option 1

ql-eec1	Synchronous digital hierarchy (SDH) Equipment Clock (0xB)
ql-prc	Primary Reference Clock (0x2)
ql-ssu-a	First Level Synchronization Supply Unit (0x4)
ql-ssu-b	Second Level Synchronization Supply Unit (0x8)
<*input*>	Enter SSM as a decimal or hexadecimal value

SSM Override Parameters for EEC Option 2

ql-eec2	Stratum 3 Traceable (0xA)
ql-prs	Stratum 1 Traceable (0x1)
ql-st2	Stratum 2 Traceable (0x7)
ql-st3e	Stratum 3E Traceable (0xD)
ql-stu	Synchronized Traceability Unknown (0x0)

ql-tnc	Transit Node Clock Traceable (0x4)
<input>	Enter SSM as a decimal or hexadecimal value

The Network Sync command set and **esmc-process** must be active for squelch to operate. Refer to the Network Sync command set on *page 4434* and the **esmc-process** command on *page 4438* for more information.

When squelch is active, the output depends on the selected format, as follows:

Format:	**Output:**
format ds1 d4	T1 AIS (unframed, all ones)
format ds1 esf	T1 AIS (unframed, all ones)
format e12 cas	E1 AIS (unframed, all ones)
format e12 ccs	E1 AIS (unframed, all ones)
format t12	none

Usage Examples

The following example enables and configures the squelch threshold as EEC option 2 **ql-tnc**:

(config)**#interface t4 0/1**
(config-t4 0/1)**#minimum-ssm-ql ql-tnc**

VDSL INTERFACE COMMAND SET

To activate the Very High-Speed Digital Subscriber Line (VDSL) Interface Configuration mode, enter the **interface vdsl** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface vdsl 1/1
(config-vdsl 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

performance-statistics on page 2496

performance-statistics

Use the **performance-statistics** command to enable gathering performance monitoring statistics on the interface. Use the **no** form of this command to disable the performance monitoring feature.

Syntax Description

No subcommands.

Default Values

By default, performance monitoring is enabled.

Command History

Release 10.10.0	Command was introduced.
Release R11.2.0	Command expanded to include the very high-speed digital subscriber line (VDSL) interfaces.

Usage Examples

The following example enables performance monitoring on the vdsl interface **vdsl 1/1**:

(config)**#interface vdsl 1/1**
(config-vdsl 1/1)**#performance-statistics**

VIRTUAL INTERFACE COMMAND SETS

This section includes the following command sets:

ATM INTERFACE COMMAND SET

To create a virtual asynchronous transfer mode (ATM) interface and/or activate the ATM Interface Configuration mode, enter the **interface atm** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface atm 1
(config-atm 1)#
```

By default, ATM interfaces are created as point-to-point links. This default setting cannot be altered. The following command creates the exact same interface as that mentioned above:

```
>enable
#configure terminal
(config)#interface atm 1 point-to-point
(config-atm 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

rtp quality-monitoring on page 2499
snmp trap on page 2500
snmp trap link-status on page 2501

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the asynchronous transfer mode (ATM) interface:

(config)**#interface atm 1**
(config-atm 1)**#rtp quality-monitoring**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP on the ATM interface:

(config)**#interface atm 1**
(config-atm 1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the ATM interface:

(config)**#interface atm 1**
(config-atm 1)**#no snmp trap link-status**

ATM SUBINTERFACE COMMAND SET

To create a virtual asynchronous transfer mode (ATM) subinterface and/or activate the ATM Subinterface Configuration mode, enter the **interface atm** command (and specify a subinterface) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface atm 1.1
(config-atm 1.1)#
```

By default, ATM subinterfaces are created as point-to-point links. This default setting cannot be altered. The following command creates the exact same interface as that mentioned above:

```
>enable
#configure terminal
(config)#interface atm 1.1 point-to-point
(config-atm 1.1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

atm routed-bridged ip on page 2504
bandwidth <value> on page 2505
bridge-group <value> on page 2506
cos on page 2507
dial-backup commands begin on page 2508
dynamic-dns on page 2525
encapsulation on page 2527
fair-queue on page 2528
hold-queue <value> out on page 2529
ip commands begin on page 2530
ipv6 dhcp relay destination <ipv6 address> on page 2575

atm routed-bridged ip

Use the **atm routed-bridged ip** command to enable IP routed bridge encapsulation (RBE) on an interface. Use the **no** form of this command to disable RBE operation.

Syntax Description

No subcommands.

Default Values

By default, RBE is disabled.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example enables RBE:

(config)**#interface atm 1.1**
(config-atm 1.1)**#atm routed-bridged ip**

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<value>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view the default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 2576*) to adjust the bandwidth appropriately for QoS configurations.

Usage Examples

The following example sets bandwidth of the ATM subinterface to 10 Mbps:

(config)**#interface atm 1.1**
(config-atm 1.1)**#bandwidth 10000**

bridge-group *<value>*

Use the **bridge-group** command to assign an interface to the specified bridge group. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<value>	Specifies the bridge group (by number) to which to assign this interface. Range is **1** to **255**.

Default Values

By default, there are no configured bridge groups.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (Ethernet to T1, Ethernet to Frame Relay subinterface).

Usage Examples

The following example assigns the ATM subinterface labeled **1.1** to bridge group **1**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#bridge-group 1**

cos

Use the **cos** command to define class of service (CoS) settings on an asynchronous transfer mode (ATM) subinterface. Use the **no** form of this command to remove the parameters. Variations of this command include:

cos ubr
cos vbr-nrt <*pcr*> <*scr*> <*mbs*>
cos vbr-rt <*pcr*> <*scr*> <*mbs*>

Syntax Description

ubr	Indicates unspecified bit rate (UBR) for the CoS.
vbr-nrt	Specifies the variable bit rate (VBR) nonreal time (NRT) peak cell rate (PCR), sustained cell rate (SCR), and maximum burst size (MBS).
vbr-rt	Specifies the variable bit rate real time (RT) peak cell rate, sustained cell rate, and maximum burst size.
<*pcr*>	Indicates the peak cell rate or maximum number of cells per second the connection can transfer into the network. Valid range is **32** to **50000** kbps.
<*scr*>	Indicates the sustained cell rate or average number of cells per second that the connection can transfer into the network. Valid range is **32** to **50000** kbps.
<*mbs*>	Indicates the maximum burst size of cells allowed on the connection. Valid range is **3** to **65535**.

Default Values

The default setting for this feature is **cos ubr**.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example defines variable bit rate real time on the ATM subinterface 1.2:

(config)**#interface atm 1.2 point-to-point**
(config-atm 1.2)**#no shutdown**
(config-atm 1.2)**#pvc 1/101**
(config-atm 1.2)**#ip address 10.23.107.35 255.255.255.240**
(config-atm 1.2)**#COS VBR-rt 2304 1024 3**
(config-atm 1.2)**#bandwidth 2304**

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the subinterface to automatically attempt a dial backup upon failure. Use the **no** form of this command to disable this feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial backup upon a failure.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example enables automatic dial backup on the endpoint:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup auto-backup**

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the subinterface to automatically discontinue dial backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures AOS to automatically restore the primary connection when the failure condition clears:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup auto-restore**

dial-backup backup-delay *<value>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

<value>	Specifies the delay period (in seconds) a failure must be active before AOS will enter backup operation on the interface. Valid range is **10** to **86400** seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures AOS to wait **60** seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup backup-delay 60**

dial-backup call-mode

Use the **dial-backup call-mode** command to specify whether the configured backup interface answers or originates (or a combination of both) backup calls. Use the **no** form of this command to return to the default value. Variations of this command include:

dial-backup call-mode answer
dial-backup call-mode answer-always
dial-backup call-mode originate
dial-backup call-mode originate-answer
dial-backup call-mode originate-answer-always

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer**.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

The majority of the configuration for AOS dial-backup implementation is configured via the dial-backup Point-to-Point Protocol (PPP) interface configuration commands. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname “Remote3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.1.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
```



```
 coding b8zs
 framing esf
 clock source line
 tdm-group 1 timeslots 1-24
 no shutdown
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.16 point-to-point
 frame-relay interface-dlci 16
 ip address 10.1.1.2 255.255.255.252
 dial-backup call-mode originate
 dial-backup number 5551111 analog ppp1
 dial-backup number 5552222 analog ppp1
no shutdown
!
interface ppp 1
 ip address 172.22.56.1 255.255.255.252
 ppp authentication chap
 username remoter outer password remoteness
 ppp chap hostname local router
 ppp chap password adtran
 no shutdown
!
ip route 192.168.2.0 255.255.255.0 172.22.56.2 255.255.255.252
!
line telnet 0 4
 password password
```

Sample configuration for central router (dialing in)

```
hostname “Central3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.100.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
 coding b8zs
 framing esf
 clock source line
```



```
 tdm-group 1 timeslots 1-24
 no shutdown
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.100 point-to-point
 frame-relay interface-dlci 100
 ip address 10.1.1.1 255.255.255.252
 dial-backup call-mode answer
 dial-backup number 555-8888 analog ppp 1
!
interface ppp 1
 ip address 172.22.56.2 255.255.255.252
 ppp authentication chap
 username local router password adtran
 ppp chap hostname remote router
 ppp chap password remoteness
 no shutdown
!
ip route 192.168.1.0 255.255.255.0 172.22.56.1 255.255.255.252

line telnet 0 4
 password password
```

Usage Examples

The following example configures AOS to generate backup calls for this endpoint using an analog modem interface (to phone number 555 1111), but never answer calls and specifies **ppp 2** as the backup interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup call-mode originate**
(config-atm 1.1)**#dial-backup number 555 1111 analog ppp 2**

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial backup, where in the configuration AOS accesses specific routing information, etc.):

Dialing Out

1. AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number on page 2518*).
3. When placing the call, AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, AOS places a call to the second number (if a second number is configured). The second number to be dialed references a separate PPP interface.

Dialing In

1. AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from caller ID, the call is terminated.

dial-backup connect-timeout <*value*>

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

<*value*>	Specifies the amount of time (in seconds) that the router will wait for a connection before attempting another call. Valid range is **10** to **300** seconds.

Default Values

By default, the **dial-backup connect-timeout** period is set to **60** seconds.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures AOS to wait **120** seconds before retrying a failed dial-backup call:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup connect-timeout 120**

dial-backup force

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*. Variations of this command include:

dial-backup force backup
dial-backup force primary

Syntax Description

backup	Forces backup regardless of primary link state.
primary	Forces primary link regardless of its state.

Default Values

By default, this feature is disabled.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures AOS to force this endpoint into dial backup:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup force backup**

dial-backup maximum-retry <*value*>

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

<*value*>	Selects the number of call retry attempts that will be made after a link failure. Valid range is **0** to **15** attempts. Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, the **dial-backup maximum-retry** period is set to **0** attempts.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures AOS to retry a dial-backup call **4** times before considering backup operation not available:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup maximum-retry 4**

dial-backup number

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. Use the **no** form of this command to disable this feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*. Variations of this command include:

dial-backup number <*number*> **analog ppp** <*interface*>
dial-backup number <*number*> **digital-56k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>
dial-backup number <*number*> **digital-64k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>

Syntax Description

<*number*>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates the number connects to an analog modem.
digital-56k	Indicates the number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates the number belongs to a digital 64 kbps per DS0 connection.
<*isdn min chan*>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
<*isdn max chan*>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
ppp <*interface*>	Specifies the Point-to-Point Protocol (PPP) interface to use as the backup for this interface (for example, **ppp 1**).

Default Values

By default, there are no configured dial-backup numbers.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.
Release 17.2	Command was expanded to include the cellular connections.
Release 17.3	Cellular connections were removed from this command.

Usage Examples

The following example configures AOS to dial **704-555-1212** (digital 64 kbps connection) to initiate dial-backup operation for this endpoint using the configured **ppp 1** backup interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup number 7045551212 digital-64k 1 1 ppp 1**

dial-backup priority <*value*>

Use the **dial-backup priority** command to select the backup priority for this interface. This allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

<*value*>	Sets the relative priority to this link. Valid range is **0** to **100**. A value of **100** designates the highest priority.

Default Values

By default, the **dial-backup priority** is set to **50**.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example assigns the highest priority to this endpoint:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup priority 100**

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

No subcommands.

Default Values

By default, AOS does not randomize the dial-backup call timers.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures AOS to randomize the dial-backup timers associated with this endpoint:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup randomize-timers**

dial-backup redial-delay <*value*>

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

<*value*>	Specifies the delay (in seconds) between attempting to redial a failed backup attempt. Valid range is **10** to **3600** seconds.

Default Values

By default, the **dial-backup redial-delay** period is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures a redial delay of **25** seconds on this endpoint:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup redial-delay 25**

dial-backup restore-delay *<value>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is bouncing in and out of alarm. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

<value>	Specifies the number of seconds AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range is **10** to **86400** seconds.

Default Values

By default, the **dial-backup restore-delay** period is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example configures AOS to wait **30** seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup restore-delay 30**

dial-backup schedule

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial backup (as specified). For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*. Variations of this command include:

dial-backup schedule day <*name*>
dial-backup schedule enable-time <*value*>
dial-backup schedule disable-time <*value*>

Syntax Description

day <*name*>	Sets the days to allow backup. Valid range is Monday through Sunday.
enable-time <*value*>	Sets the time of day to enable backup. Time is entered in a 24-hour format (00:00).
disable-time <*value*>	Sets the time of day to disable backup. Time is entered in a 24-hour format (00:00).

Default Values

By default, dial backup is enabled for all days and times if the **dial-backup auto-backup** command has been issued and the dial-backup schedule has not been entered.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example enables dial backup Monday through Friday 8:00 a.m. to 7:00 p.m.:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup schedule enable-time 08:00**
(config-atm 1.1)**#dial-backup schedule disable-time 19:00**
(config-atm 1.1)**#no dial-backup schedule day Saturday**
(config-atm 1.1)**#no dial-backup schedule day Sunday**

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2511*.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are disabled.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example deactivates the configured dial-backup interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dial-backup shutdown**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies the user name.
<*password*>	Specifies the password.
	Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#dynamic-dns dyndns-custom host user pass**

encapsulation

Use the **encapsulation** command to configure the encapsulation type for the ATM Adaptation Layer (AAL) of the Asynchronous Transfer Mode (ATM) Protocol Reference Model. Use the **no** form of this command to return to the default setting. Variations of this command include:

encapsulation aal5mux ip
encapsulation aal5mux ppp
encapsulation aal5snap

Syntax Description

aal5mux ip	Specifies encapsulation type for multiplexed virtual circuits using the IP protocol.
aal5mux ppp	Specifies encapsulation type for multiplexed virtual circuits using the Point-to-Point Protocol (PPP).
aal5snap	Specifies encapsulation type that supports LLC/SNAP protocols.

Default Values

By default, the encapsulation type is **aal5snap**.

Command History

Release 8.1	Command was introduced.

Functional Notes

For PPP and Point-to-Point Protocol over Ethernet (PPoE), the encapsulation type can be **aal5snap** or **aal5mux ppp**. For IP with no bridging, the encapsulation type can be **aal5snap** or **aal5mux ip**. For IP with bridging, the encapsulation type can only be **aal5snap**. For bridging, the encapsulation type can only be **aal5snap**.

Usage Examples

The following example sets the encapsulation type to **aal5snap**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#encapsulation aal5snap**

fair-queue

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable first in, first out (FIFO) queueing for an interface. Variations of this command include:

fair-queue
fair-queue <*value*>

WFQ must be enabled on an interface to use priority queuing. By default, WFQ is enabled for all interfaces with maximum bandwidth speeds equivalent to T1/E1 and below.

Syntax Description

<*value*>	Optional. Value that specifies the maximum number of packets that can be present in each conversation subqueue. Packets received for a conversation after this limit is reached are discarded. Range is **16** to **512** packets.

Default Values

By default, **fair-queue** is enabled with a threshold of **64** packets.

Command History

Release 5.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example enables WFQ on the interface with a threshold set at **100** packets:

(config)**#interface atm 1.1**
(config-atm 1.1)**#fair-queue 100**

hold-queue <*value*> out

Use the **hold-queue out** command to change the overall size of an interface's wide area network (WAN) output queue. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	The total number of packets the output queue can contain before packets are dropped. Range is **16** to **1000** packets.

Default Values

The default queue size for weighted fair queuing (WFQ) is **400**. The default queue size for Point-to-Point Protocol (PPP) first in, first out (FIFO) and Frame Relay round-robin is **200**.

Command History

Release 5.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example sets the overall output queue size to **700**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#hold-queue 700 out**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to create an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Specifies the assigned IPv4 ACL name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic into the ATM subinterface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface atm 1.1**
(config-atm 1.1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the ATM interface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip access-policy PRIVATE**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii <*string*> **| hex** <*value*>**] [client-id [**<*interface*> **|** <*identifier*>**]] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp client-id [<*interface*> **|** <*identifier*>**] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp hostname *"*<*string*>*"* **[no-default-route | no-domain-name | no-nameservers] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track <*name*>**] [**<*administrative distance*>**]**
ip address dhcp track <*name*> **[**<*administrative distance*>**]**

Syntax Description

<*administrative distance*>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii <*string*>	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex <*value*>	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<*interface*>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<*identifier*>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the <*identifier*> option.
hostname <*"string"*>	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

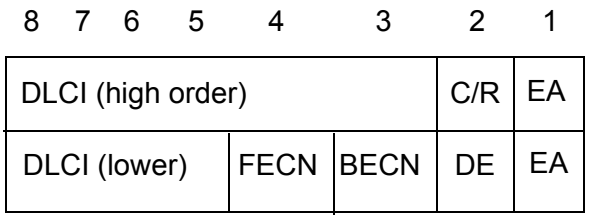
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *“<string>”* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip address dhcp hostname “adtran” no-default-route no-domain-name no-nameservers 5**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 255.255.255.252**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip address 192.22.72.101 255.255.255.252 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

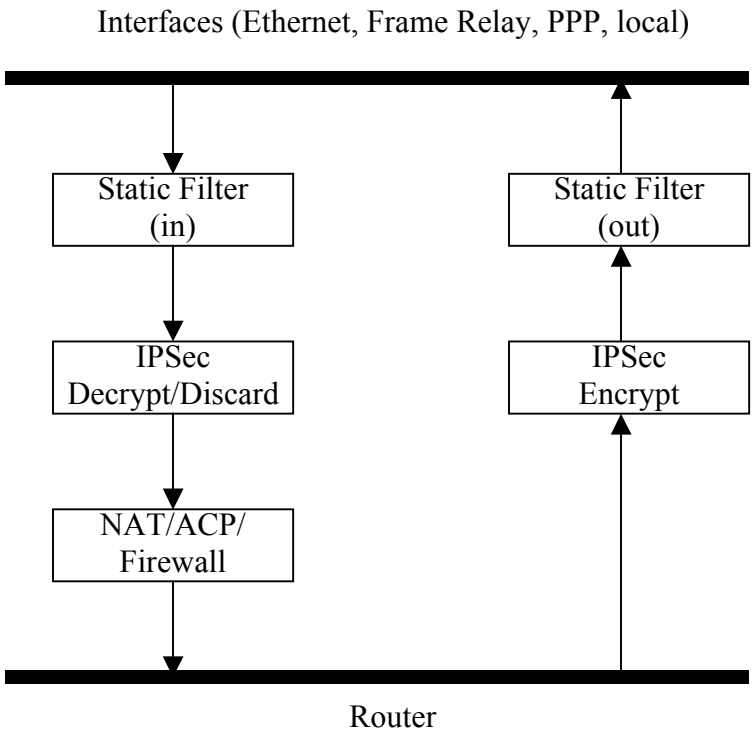
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip crypto map MyMap**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).

Usage Examples

The following example releases the IPv4 DHCP address for the ATM subinterface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip dhcp release**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast *<name>*

Syntax Description

<name>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **atm 1.1**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute Engine on this interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries on this interface to be cleared.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **8192**.

Default Values

By default, the RapidRoute Engine is disabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example enables RapidRoute and sets the maximum number of entries in the flow table to **50**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip ffe max-entries 50**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on an **atm** subinterface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign an address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (**255.255.255.255**) or a subnet broadcast (for example, **192.33.4.251** for the **192.33.4.248 /30** subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface atm 1.1**
(config-atm 1.1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP Version 2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP Version 2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP Version 2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 7.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 2554* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip mcast-stub downstream**

ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*address*> command to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface atm1.1**
(config-atm 1.1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address, ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 2551*, and *ip mcast-stub upstream on page 2554* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 2551* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the ATM subinterface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<process id>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip ospf network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is 1.

Command History

Release 11.1	Command was introduced.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the asynchronous transfer mode (ATM) subinterface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every 60 seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the asynchronous transfer mode (ATM) subinterface 1.1 every **3600** seconds:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to **300** seconds:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation delay to **300** milliseconds:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the asynchronous transfer mode (ATM) subinterface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the ATM subinterface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

Use the **ip rip receive version** to specify a RIP version that will override the **version** (in the Router RIP) configuration.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the ATM subinterface 1.1 to accept only RIP version 2 packets:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

Use the **ip rip send version** to specify a RIP version that will override the **version** (in the Router RIP) configuration.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the ATM subinterface 1.1 to transmit only RIP version 2 packets:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the ATM subinterface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the command *ip address <ipv4 address> <subnet mask> on page 2536*).

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Frame Relay Subinterface Configuration mode configures the Frame Relay subinterface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the ATM subinterface 1.1 to use the IP address assigned to the Ethernet interface (**eth 0/1**):

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip unnumbered eth 0/1**

ip urlfilter *<name>*

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the asynchronous transfer mode (ATM) subinterface 1.1 and matches the URL filter named **MyFilter**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ip urlfilter MyFilter in**

ipv6 dhcp relay destination <*ipv6 address*>

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination <*ipv6 address*>
ipv6 dhcp relay destination <*ipv6 address*> <*interface*>

Syntax Description

<*ipv6 address*>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<*interface*>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** <*ipv6 address*> **?** to display a list of valid interfaces.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the Tunnel interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command **ipv6**.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#ipv6**
(config-atm 1.1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

max-reserved-bandwidth <*value*>

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<*value*>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies **85** percent bandwidth on the asynchronous transfer mode (ATM) subinterface to be available for use in user-defined queues:

(config)**#interface atm 1.1**
(config-atm 1.1)**#max-reserved-bandwidth 85**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip secondary <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A4.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface atm 1.1**
(config-atm 1.1)**#media-gateway ip primary**

oam retry

Use the **oam retry** command to configure parameters related to operations, administration, and maintenance (OAM) management for an asynchronous transfer mode (ATM) interface. Use the **no** form of this command to disable OAM management parameters. Variations of this command include:

oam retry
oam retry *<up value>*
oam retry *<up value> <down value>*
oam retry *<up value> <down value> <value>*

Syntax Description

<up value>	Optional. Specifies the number of consecutive end-to-end F5 OAM loopback cell responses that must be received in order to change a permanent virtual circuit (PVC) connection state to up. Range is **1** to **255**.
<down value>	Optional. Specifies the number of consecutive end-to-end F5 OAM loopback cell responses that are not received in order to change a PVC state to down. Range is **1** to **255**.
<value>	Optional. Specifies the frequency (in seconds) that end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state of a PVC is being verified. Range is **1** to **600** seconds.

Default Values

By default, the up-count is set to 3, the down-count is set to 5, and the retry frequency is 1.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example configures the OAM parameters with an up-count of **2**, down-count of **2**, and retry frequency of **10**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#oam retry 2 2 10**

oam-pvc managed

Use the **oam-pvc managed** command to enable end-to-end F5 operations, administration, and maintenance (OAM) loopback cell generation and OAM management for an asynchronous transfer mode (ATM) interface. Use the **no** form of this command to disable generation of OAM loopback cells. Variations of this command include:

oam-pvc managed
oam-pvc managed <*value*>

Syntax Description

<*value*>	Optional. Specifies the time delay between transmitting OAM loopback cells. Range is **0** to **600** seconds.

Default Values

By default, the frequency is 1 second.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example enables OAM loopback cell generation with a frequency of **5** seconds:

(config)**#interface atm 1.1**
(config-atm 1.1)**#oam-pvc managed 5**

packet-capture <*name*>

Use the **packet-capture** command to apply a previously configured packet capture instance to the interface. Use the **no** form of this command to remove the packet capture instance.

Syntax Description

<*name*>	Specifies the name of the packet capture instance to apply to the interface.

Default Values

By default, no packet capture instances are configured or applied to the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. For more information about packet capturing, its uses, and its implementation in AOS, refer to the configuration guide *Configuring Packet Capture in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example applies the previously configured packet capture **1CAPTURE** to the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#packet-capture 1CAPTURE**

pvc <*VPI/VCI*>

Use the **pvc** command to select the asynchronous transfer mode (ATM) virtual link for this subinterface. Use the **no** form of this command to remove the link.

Syntax Description

<*VPI/VCI*>	Specifies the ATM network virtual path identifier (VPI) for this permanent virtual circuit (PVC). The VPI value range is **0** to **255**, and the virtual channel identifier (VCI) value range is **32** to **65535**.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example sets the VPI to **8** and the VCI to **35**:

(config)**#interface atm 1.1**
(config-atm 1.1)**#pvc 8/35**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.
Release 15.1	Command was expanded to include the **in** parameter.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing (WFQ).
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the ATM subinterface 1.1:

(config)**#interface atm 1.1**
(config-atm 1.1)**#qos-policy out VOICEMAP**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.9	Command was expanded to the Frame Relay and the ATM subinterfaces.

Usage Examples

The following example enables SNMP on the virtual ATM subinterface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.9	Command was explanded to the Frame Relay and the ATM subinterfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on th ATM subinterface:

(config)**#interface atm 1.1**
(confi-atm 1.1)**#no snmp trap link-status**

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** command to block bridge protocol data units (BPDUs) from being transmitted and received on this interface. To return to the default value, use the **no** form of this command. Variations of this command include:

spanning-tree bpdufilter disable
spanning-tree bpdufilter enable

Syntax Description

disable	Disables the BPDU filter.
enable	Enables the BPDU filter.

Default Values

By default, this command is set to **disable**.

Command History

Release 5.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

The purpose of this command is to remove a port from participation in the spanning tree. This might be beneficial while debugging a network setup. It normally should not be used in a live network.

Usage Examples

The following example enables the BPDU filter on the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#spanning-tree bpdufilter enable**

spanning-tree bpduguard

Use the **spanning-tree bpduguard** command to block bridge protocol data units (BPDUs) from being received on this interface. To return to the default value, use the **no** form of this command. Variations of this command include:

spanning-tree bpduguard disable
spanning-tree bpduguard enable

Syntax Description

disable	Disables the BPDU block.
enable	Enables the BPDU block.

Default Values

By default, this command is set to **disable**.

Command History

Release 5.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Usage Examples

The following example enables the bpduguard on the interface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#spanning-tree bpduguard enable**

spanning-tree edgeport

Use the **spanning-tree edgeport** command to set this interface to be an edgeport. This command overrides the global setting (refer to *spanning-tree edgeport default on page 1837*). Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, this command is set to disable.

Command History

Release 5.1	Command was introduced.
Release 8.1	Command was added to the ATM Subinterface command set.

Functional Notes

When an interface is designated as an edgeport, the interface will immediately go to a forwarding state when the link becomes active. When an interface is not designated as an edgeport, the interface must go through the listening and learning states before going to the forwarding state.

Usage Examples

The following example configures the interface to be an edgeport:

(config)**#interface atm 1.1**
(config-atm 1.1)**#spanning-tree edgeport**

An individual interface can be configured to not be considered an edgeport. For example:

(config)**#interface atm 1.1**
(config-atm 1.1)**#spanning-tree edgeport disable**

or

(config)**#interface atm 1.1**
(config-atm 1.1)**#no spanning-tree edgeport**

spanning-tree link-type

Use the **spanning-tree link-type** command to configure the spanning-tree protocol link type for an interface. To return to the default value, use the **no** form of this command. Variations of this command include:

spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared

Syntax Description

auto	Determines link type by the port's duplex settings.
point-to-point	Sets link type manually to point-to-point regardless of duplex settings.
shared	Sets link type manually to shared regardless of duplex settings.

Default Values

By default, a port is set to auto.

Command History

Release 5.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

This command overrides the default link-type setting determined by the duplex of the individual port. By default, a port configured for half-duplex is set to **shared** link type, and a port configured for full-duplex is set to **point-to-point** link type. Setting the link type manually overrides the default and forces the port to use the specified link type. Using the **link-type auto** command, restores the convention of determining link type based on duplex settings.

Usage Examples

The following example forces the link type to point-to-point, even if the port is configured to be half-duplex:

(config)**#bridge 1 protocol ieee**
(config)**#interface atm 1.1**
(config-atm 1.1)**#spanning-tree link-type point-to-point**

Technology Review

Rapid transitions are possible in Rapid Spanning Tree Protocol (RSTP) by taking advantage of point-to-point links (a port is connected to exactly one other bridge) and edge-port connections (a port is not connected to any additional bridges). Setting the link type to **auto** allows the spanning tree to automatically configure the link type based on the duplex of the link. Setting the link type to **point-to-point** allows a half-duplex link to act as if it were a point-to-point link.

spanning-tree path-cost *<value>*

Use the **spanning-tree path-cost** command to assign a cost to a bridge group that is used when computing the spanning-tree root path. To return to the default path-cost value, use the **no** form of this command.

Syntax Description

<value>	Assigns a number to the bridge interface to be used as the path cost in spanning calculations. Valid range is **0** to **65535**.

Default Values

By default, the path-cost value is set to 19.

Command History

Release 1.1	Command was introduced.
Release 8.1	Command was added to the ATM subinterface command set.
Release R10.1.0	Command was added to the Ethernet interface command set.

Functional Notes

The specified value is inversely proportional to the likelihood the bridge interface will be chosen as the root path. Set the path-cost value lower to increase the chance the interface will be the root. To obtain the most accurate spanning-tree calculations, develop a system for determining path costs for links and apply it to all bridged interfaces.

Usage Examples

The following example assigns a path cost of 100 for bridge group 17 on an ATM subinterface:

(config)**#interface atm 1.1**
(config-atm 1.1)**#spanning-tree path-cost 100**

Technology Review

Spanning-tree protocol provides a way to prevent loopback or parallel paths in bridged networks. Using the priority values and path costs assigned to each bridging interface, the spanning-tree protocol determines the root path and identifies whether to block or allow other paths.

spanning-tree port-priority <*value*>

Use the **spanning-tree port-priority** command to select the priority level of a port associated with a bridge. To return to the default bridge-group priority value, use the **no** form of this command.

Syntax Description

<*value*>	Assigns a priority value for the bridge group; the lower the value, the higher the priority. Valid range is **0** to **255**.

Default Values

By default, the bridge-group priority value is set to 128.

Command History

Release 1.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.

Functional Notes

The only time that this priority level is used is when two interfaces with a path to the root have equal cost. At that point, the level set in this command will determine which port the bridge will use. Set the priority value lower to increase the chance the interface will be used.

Usage Examples

The following example sets the maximum priority on the ATM subinterface labeled 1.1 in bridge group 17:

(config)**#interface atm 1.1**
(config-atm 1.1)**#spanning-tree port-priority 0**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the ATM subinterface labeled 1.1 to the VRF instance named **RED**:

(config)**#interface atm 1.1**
(config-fr 1.16)**#vrf forwarding RED**

BVI INTERFACE COMMAND SET

To activate the Bridged Virtual Interface Configuration mode, first enable integrated routing and bridging (IRB) via the **bridge irb** command (refer to *bridge irb on page 1229*) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#bridge irb
```

Next, enter the **interface bvi** command and a specific interface number that corresponds to an existing bridge group at the Global Configuration mode prompt. For example:

```
(config)#bridge irb
(config)#interface bvi 1
(config-bvi 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81M
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bandwidth <value> on page 2594
dynamic-dns on page 2595
ip commands begin on page 2597
ipv6 dhcp relay destination <ipv6 address> on page 2628
mac-address <mac address> on page 2629
max-reserved-bandwidth <value> on page 2630
packet-capture <name> on page 2631
qos-policy out <name> on page 2632
rtp quality-monitoring on page 2633
traffic-shape rate <value> on page 2634
vrf forwarding <name> on page 2635

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<value>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 2630*) to adjust the bandwidth appropriately for QoS configurations.

Usage Examples

The following example sets bandwidth of BVI 1 to 10 Mbps:

(config)**#interface bvi 1**
(config-bvi 1)**#bandwidth 10000**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface bvi 1**
(config-bvi 1)**#dynamic-dns dyndns-custom host user pass**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to create an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Specifies the IPv4 ACL name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic into BVI 1:

(config)**#interface bvi 1**
(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config)**#interface bvi 1**
(config-bvi 1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the BVI interface 1:

(config)**#interface bvi 1**
(config-bvi 1)**#ip access-policy PRIVATE**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

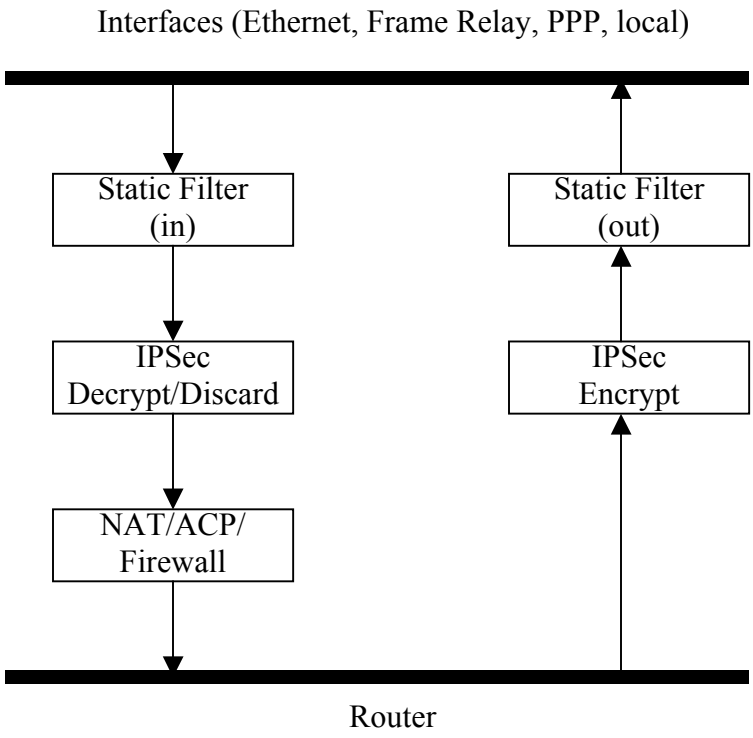
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#interface bvi 1**
(config-bvi 1)**#ip crypto map MyMap**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii *<string>* **| hex** *<value>***] [client-id [***<interface>* **|** *<identifier>***]] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp client-id [*<interface>* **|** *<identifier>***] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp hostname *"<string>"* **[no-default-route | no-domain-name | no-nameservers] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track *<name>***] [***<administrative distance>***]**
ip address dhcp track *<name>* **[***<administrative distance>***]**

Syntax Description

<administrative distance>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii *<string>*	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex *<value>*	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<interface>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<identifier>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the *<identifier>* option.
hostname *<"string">*	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

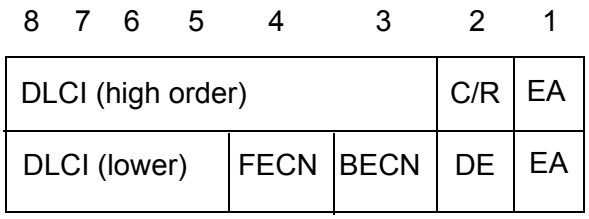
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *“<string>”* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#interface bvi 1**
(config-bvi 1)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#interface bvi 1**
(config-bvi 1)**#ip address dhcp hostname “adtran” no-default-route no-domain-name no-nameservers 5**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 255.255.255.252**:

(config)**#interface bvi 1**
(config-bvi 1)**#ip address 192.22.72.101 255.255.255.252 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface bvi 1**
(config-bvi 1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).

Usage Examples

The following example releases the DHCP IPv4 address for the virtual interface:

(config)**#interface bvi 1**
(config-bvi 1)**#ip dhcp release**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface bvi 1**
(config-bvi 1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on BVI 1:

(config)**#interface bvi 1**
(config-bvi 1)**#ip directed-broadcast**

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on a bridged virtual interface (BVI) to monitor incoming traffic through an ACL called **myacl**:

(config)**#interface bvi 1**
(config-bvi 1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper-address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248 /30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface bvi 1**
(config-bvi 1)**#ip helper-address 192.33.5.99**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface bvi 1**
(config-bvi 1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release 15.1	Command was expanded to include the BVIs.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface bvi 1**
(config-bvi 1)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<process id>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on BVI 1:

(config)**#interface bvi 1**
(config-bvi 1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release 15.1	Command was expanded to include the BVIs.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface bvi 1**
(config-bvi 1)**#ip ospf 1 network broadcast**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

(config)**#interface bvi 1**
(config-bvi 1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on BVI 1:

(config)**#interface bvi 1**
(config-bvi 1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that will override the **version** (in the Router RIP) configuration.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures a BVI to accept only RIP version 2 packets:

(config)**#interface bvi 1**
(config-bvi 1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

Use the **ip rip send version** to specify a RIP version that will override the **version** (in the Router RIP) configuration.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures a BVI to transmit only RIP version 2 packets:

(config)**#interface bvi 1**
(config-bvi 1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface bvi 1**
(config-bvi 1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual bridged virtual interfaces (BVIs). IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.
Release 15.1	Command was expanded to include the BVIs.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast-cache switching on a BVI:

(config)**#interface bvi 1**
(config-bvi 1)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the BVI Configuration mode configures the BVI to use the IP address assigned to the Ethernet interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures BVI 1 to use the IP address assigned to the Ethernet interface (**eth 0/1**):

(config)**#interface bvi 1**
(config-bvi 1)**#ip unnumbered eth 0/1**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through BVI 1 and matches the URL filter named **MyFilter**:

(config)**#interface bvi 1**
(config-bvi 1)**#ip urlfilter MyFilter in**

ipv6 dhcp relay destination *<ipv6 address>*

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination *<ipv6 address>*
ipv6 dhcp relay destination *<ipv6 address> <interface>*

Syntax Description

<ipv6 address>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** *<ipv6 address>* **?** to display a list of valid interfaces.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the Tunnel interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command **ipv6**.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface bvi 1**
(config-bvi 1)**#ipv6**
(config-bvi 1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

mac-address *<mac address>*

Use the **mac-address** command to specify the medium access control (MAC) address of the virtual local area network (VLAN) interface. Only the last three values of the MAC address can be modified. The first three values contain the Adtran reserved number (00:0A:C8) by default. Use the **no** form of this command to return to the default MAC address programmed by Adtran.

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

A unique default MAC address is programmed in each unit shipped by Adtran.

Command History

Release 5.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Usage Examples

The following example configures a MAC address of **00:0A:C8:5F:00:D2** for BVI 1:

(config)**#interface bvi 1**
(config-bvi 1)**#mac-address 00:0A:C8:5F:00:D2**

max-reserved-bandwidth *<value>*

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<value>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Usage Examples

The following example specifies **85** percent of the bandwidth on BVI 1 be available for use in user-defined queues:

(config)**#interface bvi 1**
(config-bvi 1)**#max-reserved-bandwidth 85**

packet-capture <*name*>

Use the **packet-capture** command to apply a previously configured packet capture instance to the interface. Use the **no** form of this command to remove the packet capture instance.

Syntax Description

<*name*>	Specifies the name of the packet capture instance to apply to the interface.

Default Values

By default, no packet capture instances are configured or applied to the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. For more information about packet capturing, its uses, and its implementation in AOS, refer to the configuration guide *Configuring Packet Capture in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example applies the previously configured packet capture **1CAPTURE** to the interface:

(config)**#interface bvi 1**
(config-bvi 1)**#packet-capture 1CAPTURE**

qos-policy out *<name>*

Use the **qos-policy out** command to apply a previously configured quality of service (QoS) map to outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface.

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing (WFQ).
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to BVI 1:

(config)**#interface bvi 1**
(config-bvi 1)**#qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the bridged virtual interface (BVI) 1:

```
(config)#interface bvi 1
(config-bvi 1)#rtp quality-monitoring
```

traffic-shape rate <*value*>

Use the **traffic-shape rate** command to specify and enforce an output bandwidth for the bridged virtual interface (BVI). Use the **no** form of this command to disable this feature. Variations of this command include:

traffic-shape rate <*value*>
traffic-shape rate <*value*> **count-eth-overhead**
traffic-shape rate <*value*> <*burst*>
traffic-shape rate <*value*> <*burst*> **count-eth-overhead**

Syntax Description

<*value*>	Specifies the rate (in bits per second) at which the interface should be shaped.
<*burst*>	Optional. Specifies the allowed burst in bytes. By default, the burst is specified as the rate divided by 5 and represents the number of bytes that would flow within 200 ms.
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.

Default Values

By default, **traffic-shape rate** is disabled.

Command History

Release 10.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release R11.1.0	Command was expanded to include the **count-eth-overhead** parameter, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

Traffic shaping can be used to limit the virtual local area network (VLAN) interface to a particular rate or to specify use of quality of service (QoS).

Usage Examples

The following example sets the outbound rate of BVI 1 to 128 kbps and applies a QoS policy that gives all Realtime Transport Protocol (RTP) traffic priority over all other traffic:

(config)**#qos map voip 1**
(config-qos-map)**#match ip rtp 10000 10500 all**
(config-qos-map)**#priority unlimited**
(config-qos-map)**#interface bvi 1**
(config-bvi 1)**#traffic-shape rate 128000**
(config-bvi 1)**#qos-policy out voip**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the **bvi 1** interface to the VRF instance named **RED**:

(config)**#interface bvi 1**
(config-bvi 1)**#vrf forwarding RED**

DEMAND INTERFACE COMMAND SET

To create a virtual demand interface and/or activate the Demand Interface Configuration mode, enter the **interface demand** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface demand 1
(config-demand 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bandwidth <value> on page 2638
called-number <number> on page 2639
caller-number <number> on page 2640
connect-mode on page 2641
connect-order on page 2642
connect-sequence on page 2643
connect-sequence attempts <value> on page 2645
connect-sequence interface-recovery on page 2646
demand-hold-queue <number> timeout <value> on page 2647
dynamic-dns on page 2648
fair-queue on page 2650
fast-idle <value> on page 2651
hold-queue <value> out on page 2652
idle-timeout <value> on page 2653
ip commands begin on page 2654
keepalive <value> on page 2689
lldp receive on page 2690
lldp send on page 2691

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies the bandwidth value in kbps.

Default Values

To view default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 2694*) to adjust the bandwidth appropriately for QoS configurations.

Usage Examples

The following example sets the bandwidth of the demand interface to 10 Mbps:

(config)**#interface demand 1**
(config-demand 1)**#bandwidth 10000**

called-number *<number>*

Use the **called-number** command to link calls to specific interfaces based on their dialed number identification service (DNIS) numbers. Multiple called numbers may be specified for an interface. Use the **no** form of this command to restore the default value.

Syntax Description

<number>	Identifies the called number to be linked to an interface. The DNIS number is limited to 20 digits.

Default Values

By default, no called numbers are defined.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example links calls with a DNIS number of **2565558409** to the demand interface **1**:

(config)**#interface demand 1**
(config-demand 1)**#called-number 2565558409**

caller-number <*number*>

Use the **caller-number** command to link calls to specific interfaces based on its caller ID (CLID) number. Multiple caller ID numbers may be specified, allowing the interface to accept calls from different remote resources. Use the **no** form of this command to restore the default value.

Syntax Description

<*number*>	Identifies the caller's number to be linked to an interface. The CLID number is limited to 20 digits.

Default Values

By default, no caller numbers are defined.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example links calls with a CLID number of **2565559911** to the demand interface **1**:

(config)**#interface demand 1**
(config-demand 1)**#caller-number 2565559911**

connect-mode

Use the **connect-mode** command to configure the interface to only answer calls, only originate calls, or to both answer and originate calls. Use the **no** form of this command to restore the default value. Variations of this command include:

connect-mode answer
connect-mode either
connect-mode originate

Syntax Description

answer	Specifies the interface may be used to answer calls, but not originate calls.
either	Specifies the interface may be used to answer and originate calls.
originate	Specifies the interface may be used to originate calls, but not answer calls.

Default Values

By default, the connect mode is set to both answer and originate calls.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to only answer calls:

(config)**#interface demand 1**
(config-demand 1)**#connect-mode answer**

connect-order

Use the **connect-order** command to specify the starting point in the connection sequence for each sequence activation. The connection sequence is a circular list. Use the **no** form of this command to restore the default value. Variations of this command include:

connect-order last-successful
connect-order round-robin
connect-order sequential

Syntax Description

last-successful	Specifies the connect sequence be processed beginning with the last successful entry or the first entry if there are no previous connections.
round-robin	Specifies the connect sequence be processed beginning with the entry that follows the last successful entry or the first entry if there are no previous connections.
sequential	Specifies the connect sequence be processed from the beginning of the list.

Default Values

By default, connect sequences are processed sequentially.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the connection sequence to begin with the last successful entry:

(config)**#interface demand 1**
(config-demand 1)**#connect-order last-successful**

connect-sequence

Use the **connect-sequence** command to provide instructions to the interface on how to use the resource pool and telephone numbers to connect to demand destinations. Use the **no** form of this command to restore the default value.Variations of this command include the following:

connect-sequence <*value*> **dial-string** <*string*> **forced-analog**
connect-sequence <*value*> **dial-string** <*string*> **forced-analog busyout-threshold** <*value*>
connect-sequence <*value*> **dial-string** <*string*> **forced-cellular**
connect-sequence <*value*> **dial-string** <*string*> **forced-cellular busyout-threshold** <*value*>
connect-sequence <*value*> **dial-string** <*string*> **forced-isdn-56k**
connect-sequence <*value*> **dial-string** <*string*> **forced-isdn-56k busyout-threshold** <*value*>
connect-sequence <*value*> **dial-string** <*string*> **forced-isdn-64k**
connect-sequence <*value*> **dial-string** <*string*> **forced-isdn-64k busyout-threshold** <*value*>
connect-sequence <*value*> **dial-string** <*string*> **isdn-56k**
connect-sequence <*value*> **dial-string** <*string*> **isdn-56k busyout-threshold** <*value*>
connect-sequence <*value*> **dial-string** <*string*> **isdn-64k**
connect-sequence <*value*> **dial-string** <*string*> **isdn-64k busyout-threshold** <*value*>

Syntax Description

<*value*>	Specifies the sequence number for this connection specification entry. Range is **1** to **65535**.
dial-string <*string*>	Specifies the telephone number to dial when using this connection. The dial string is limited to 20 digits.
forced-analog	Specifies that only analog resources may be used.
forced-cellular	Specifies that only cellular resources may be used.
forced-isdn-56k	Specifies that only integrated services digital network (ISDN) resources may be used. Call is placed using ISDN 56k.
forced-isdn-64k	Specifies that only ISDN resources may be used. Call is placed using ISDN 64k.
isdn-56k	Specifies any dial resource may be used if ISDN 56k call type is used.
isdn-64k	Specifies any dial resource may be used if ISDN 64k call type is used.
busyout-threshold <*value*>	Optional. Specifies the maximum number of connect sequence cycles during an activation attempt that must fail before it is skipped until the next activation attempt.

Default Values

By default, any dial resource may be used.

By default, the dial string for cellular connections is **#777**.

Command History

Release 11.1	Command was introduced.
Release 17.2	Command was expanded to include the cellular connections.

Usage Examples

The following example instructs demand interface **1** to place the call using ISDN 64k:

(config)**#interface demand 1**
(config-demand 1)**#connect-sequence 65 dial-string 2565559911 forced-isdn-64k**

The following example instructs demand interface 1 to place the call using a cellular connection:

(config)**#interface demand 1**
(config-demand 1)**#connect-sequence 1 dial-string #777 forced-cellular**

connect-sequence attempts *<value>*

Use the **connect-sequence attempts** command to limit the number of times the connect sequence will cycle when its entries are unable to establish a connection. When the maximum number of attempts are exhausted, the interface will go into recovery mode. Refer to *connect-sequence interface-recovery on page 2646* for more information. Use the **no** form of this command to restore the default value.

Syntax Description

<value>	Specifies the number of times the connect sequence will cycle through its entries if it is unable to make a connection. Range is **0** to **65535**.

Default Values

By default, the **connect-sequence attempts** are unlimited.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs demand interface **1** to attempt its connection sequence **500** times:

(config)**#interface demand 1**
(config-demand 1)**#connect-sequence attempts 500**

connect-sequence interface-recovery

Use the **connect-sequence interface-recovery** command to allow the interface to go down in the event that the **connect-sequence attempts** value is exhausted. Refer to *connect-sequence attempts <value> on page 2645* for more information. Use the **no** form of this command to restore the default value. Variations of this command include:

connect-sequence interface-recovery
connect-sequence interface-recovery retry-interval <*value*>
connect-sequence interface-recovery retry-interval <*value*> **max-retries** <*number*>

Syntax Description

retry-interval <*value*>	Optional. Specifies the number of seconds the interface will wait between connect sequence cycles during recovery attempts.
max-retries <*number*>	Optional. Specifies the maximum number of times the connect sequence will cycle in an attempt to bring the interface back up. When in interface recovery mode, this value overrides the **connect-sequence attempts** value.

Default Values

By default, the **connect-sequence interface-recovery retry-interval** is set to 120 seconds and **max-retries** are unlimited.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to wait **60** seconds between retry attempts with a maximum number of **500** retries:

(config)**#interface demand 1**
(config-demand 1)**#connect-sequence interface-recovery retry-interval 60 max-retries 500**

demand-hold-queue <*number*> timeout <*value*>

Use the **demand-hold-queue timeout** command to set the number and length of time interesting packets will be held while a connection is being made. Use the **no** form of this command to restore the default value.

Syntax Description

<*number*>	Specifies the number of packets that may be stored in the hold queue. Range is **0** to **100**.
<*value*>	Specifies the number of seconds a packet may remain in the hold queue. Range is **0** to **255** seconds.

Default Values

By default, the hold queue is disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to hold **50** packets in the queue for up to **120** seconds:

(config)**#interface demand 1**
(config-demand 1)**#demand-hold-queue 50 timeout 120**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface demand 1**
(config-demand 1)**#dynamic-dns dyndns-custom host user pass**

fair-queue

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable first in, first out (FIFO) queueing for an interface. Variations of this command include:

fair-queue
fair-queue <*threshold*>

WFQ must be enabled on an interface to use priority queuing. By default, WFQ is enabled for all interfaces with maximum bandwidth speeds equivalent to T1/E1 and below.

Syntax Description

<*threshold*>	Optional. Specifies the maximum number of packets that can be present in each conversation subqueue. Packets received for a conversation after this limit is reached are discarded. Range: **16** to **512** packets.

Default Values

By default, WFQ is enabled with a threshold of 64 packets.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Usage Examples

The following example enables WFQ on the interface with a threshold set at 100 packets:

(config)**#interface demand 1**
(config-demand 1)**#fair-queue 100**

fast-idle *<value>*

Use the **fast-idle** command to set the amount of time the demand interface connection will remain active in the absence of interesting traffic when there is contention for the demand resources being used by this interface. Use the **no** form of this command to restore the default value.

Syntax Description

<value>	Specifies the number of seconds the interface will remain up in the absence of interesting traffic. Range is **1** to **2147483** seconds.

Default Values

By default, **fast-idle** is set to 120 seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets fast idle to **1073752** seconds:

(config)**#interface demand 1**
(config-demand 1)**#fast-idle 1073752**

hold-queue <*value*> out

Use the **hold-queue out** command to change the overall size of an interface's wide area network (WAN) output queue. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the total number of packets the output queue can contain before packets are dropped. Range is **16** to **1000** packets.

Default Values

The default queue size for weighted fair queuing (WFQ) is **400**. The default queue size for Point-to-Point Protocol (PPP) first in, first out (FIFO) and Frame Relay round-robin is **200**.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Usage Examples

The following example sets the overall output queue size to **700**:

(config)**#interface demand 1**
(config-demand 1)**#hold-queue 700 out**

idle-timeout <*value*>

Use the **idle-timeout** command to set the amount of time the interface link/bundle will remain up in the absence of interesting traffic. Interesting traffic and direction logic are set using the **match-interesting** commands. Refer to *match-interesting ip on page 2693* for more information. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies the number of seconds the interface will remain up in the absence of interesting traffic. Range is **1** to **2147483** seconds.

Default Values

By default, **idle-timeout** is set to **120** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to time out after **360** seconds:

(config)**#interface demand 1**
(config-demand 1)**#idle-timeout 360**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to create an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Indicates the assigned IPv4 ACL name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic into the demand interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface demand 1**
(config-demand 1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the deman interface 1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the demand interface 1:

(config)**#interface demand 1**
(config-demand 1)**#ip access-policy PRIVATE**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the optional keyword **secondary** to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 255.255.255.252**:

(config)**#interface demand 1**
(config-demand 1)**#ip address 192.22.72.101 255.255.255.252 secondary**

ip address cellular

Use the **ip address cellular** command to allow the interface to be assigned an IP address and name server from a cellular modem. Use the **no** form of this command to disable the feature. Variations of this command include:

ip address cellular
ip address cellular no-nameservers

Syntax Description

no-nameservers	Optional. Specifies that the interface receives an IP address from a cellular modem but does not receive a name server.

Default Values

By default, the interface is assigned an address with the command *ip address <ipv4 address> <subnet mask> on page 2657*.

Command History

Release 11.9.0	Command was introduced.

Functional Notes

In order to configure the demand interface using the **ip address cellular** command, you must also configure the interface to use High Level Data Link Control (HDLC) encapsulation, have a cellular resource configured in the resource pool, and configure the **connect-sequence** to use **forced-cellular**. In addition, for interesting traffic to arrive at the demand interface, a static route must be configured on the AOS device. The following configuration example displays the necessary configurations for this command to be used:

(config)**#interface demand 1 encapsulation hdlc**
(config-demand 1)**#resource pool LTERESOURCE**
(config-demand 1)**#connect-sequence 1 dial-string #777 forced-cellular**
(config-demand 1)**#ip address cellular**
(config-demand 1)**#exit**
(config)**#ip route 0.0.0.0 0.0.0.0 demand 1**

Usage Examples

The following example enables the demand interface to receive an IP address and name server from a cellular modem:

(config)**#interface demand 1**
(config-demand 1)**#ip address cellular**

ip address negotiated

Use the **ip address negotiated** command to allow the interface to negotiate (i.e., be assigned) an IP address from the far-end Point-to-Point Protocol (PPP) connection. Use the **no** form of this command to disable the negotiation for an IP address. Variations of this command include:

ip address negotiated
ip address negotiated dns-sync
ip address negotiated dns-sync no-default
ip address negotiated no-default
ip address negotiated no-default dns-sync

Syntax Description

dns-sync	Optional. Specifies that when the IP address is negotiated, domain naming system (DNS) information is also received.
no-default	Optional. Prevents the insertion of a default route. Some systems already have a default route configured and need a static route to the PPP interface to function correctly.

Default Values

By default, the interface is assigned an address with the **ip address** <*ip address*> <*subnet mask*> command.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was expanded to include the **dns-sync** parameter.

Usage Examples

The following example enables the demand interface to negotiate an IP address from the far-end connection:

(config)**#interface demand 1**
(config-demand 1)**#ip address negotiated**

The following example enables the demand interface to negotiate an IP address from the far-end connection without inserting a default route:

(config)**#interface demand 1**
(config-demand 1)**#ip address negotiated no-default**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface demand 1**
(config-demand 1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

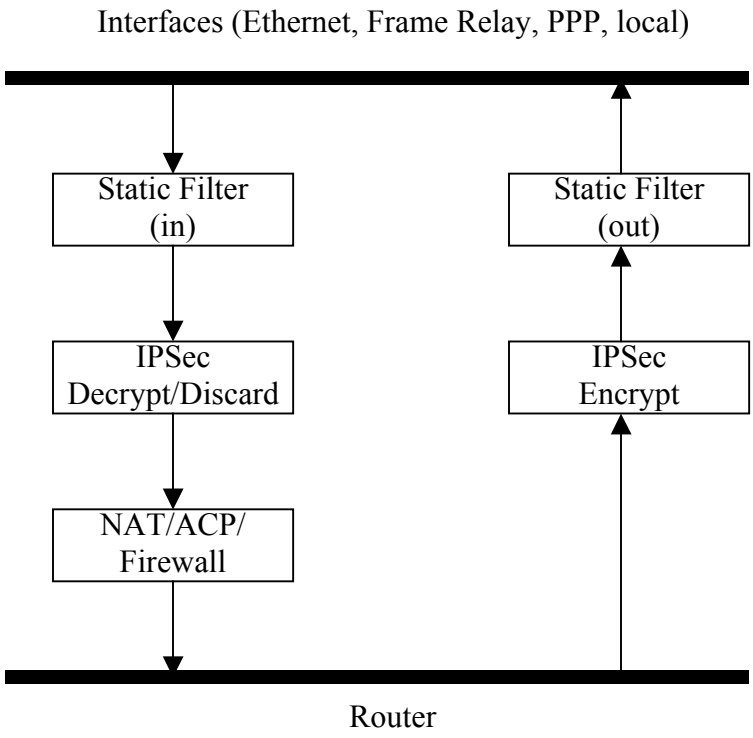
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#demand 1**
(config-demand 1)**#ip crypto map MyMap**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface demand 1**
(config-demand 1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast *<name>*

Syntax Description

<name>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **demand 1**:

(config)**#interface demand 1**
(config-demand 1)**#ip directed-broadcast**

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on a **demand** interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface demand 1**
(config-demand 1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (**255.255.255.255**) or a subnet broadcast (for example, **192.33.4.251** for the **192.33.4.248 /30** subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface demand 1**
(config-demand 1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description (Continued)

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 7.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface demand 1**
(config-demand 1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 2674* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

(config)**#interface demand 1**
(config-demand 1)**#ip mcast-stub downstream**

ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the command *ip igmp on page 2669* to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface demand 1**
(config-demand 1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 2671*, and *ip mcast-stub upstream on page 2674* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface demand 1**
(config-demand 1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 2671* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

(config)**#interface demand 1**
(config-demand 1)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface demand 1**
(config-demand 1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface demand 1**
(config-demand 1)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the demand interface:

(config)**#interface demand 1**
(config-demand 1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface demand 1**
(config-demand 1)**#ip ospf 1 network broadcast**

ip policy route-map *<name>*

Use the **ip policy route-map** command to associate a route map with a network interface source. Use the **no** form of this command to disable this feature.

Syntax Description

<name>	Specifies the route map to associate with this interface.

Default Values

By default, policy-based routing is disabled for all interfaces.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example associates the route map named **MyMap** with demand interface **1**:

(config)**#interface demand 1**
(config-demand 1)**#ip policy route-map MyMap**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the virtual demand interface:

(config)**#interface demand 1**
(config-demand 1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

Use the **ip rip receive version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual demand interface to accept only RIP version 2 packets:

(config)**#interface demand 1**
(config-demand 1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

Use the **ip rip send version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual demand interface to transmit only RIP version 2 packets:

(config)**#interface demand 1**
(config-demand 1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface demand 1**
(config-demand 1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual demand interfaces.

Command History

Release 2.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

Fast-cache switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast-cache switching on the virtual demand interface:

(config)**#interface demand 1**
(config-demand 1)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Demand Interface Configuration mode configures the demand interface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface. Static routes may either use the interface name (ppp 1) or the far-end address (if it will be discovered).

Usage Examples

The following example configures the demand interface (labeled **demand 1**) to use the IP address assigned to the Ethernet interface (**eth 0/1**):

(config)**#interface demand 1**
(config-demand 1)**#ip unnumbered eth 0/1**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the demand interface (labeled **demand 1**) and matches the URL filter named **MyFilter**:

(config)**#interface demand 1**
(config-demand 1)**#ip urlfilter MyFilter in**

keepalive *<value>*

Use the **keepalive** command to enable the transmission of keepalive packets on the interface and specify the time interval in seconds between transmitted packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Defines the time interval (in seconds) between transmitted keepalive packets. Range is **0** to **32767** seconds.

Default Values

By default, the time interval between transmitted keepalive packets is **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

If three keepalive packets are sent to an interface with no response, the interface is considered down. To detect interface failures quickly, specify a smaller keepalive time.

Usage Examples

The following example specifies a keepalive time of 5 seconds on the virtual demand interface:

(config)**#interface demand 1**
(config-demand 1)**#keepalive 5**

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 9.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Usage Examples

The following example configures the demand interface to receive LLDP packets:

(config)**#interface demand 1**
(config-demand 1)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to disable this feature. Variations of this command include:

lldp send
lldp send management-address
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

By default, all interfaces are configured to transmit and receive LLDP packets of all types.

Command History

Release 9.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the demand interface to transmit LLDP packets containing all enabled information types:

(config)**#interface demand 1**
(config-demand 1)**#lldp send**

The following example configures the demand interface to transmit and receive LLDP packets containing all information types:

(config)**#interface demand 1**
(config-demand 1)**#lldp send-and-receive**

match-interesting ip

Use the **match-interesting ip** command to allow an access control list (ACL) to specify which traffic attempting to cross this interface will be considered interesting. Use the **no** form of this command to restore the default value. Variations of this command include:

match-interesting ip list <*name*>
match-interesting ip list <*name*> **in**
match-interesting ip list <*name*> **out**
match-interesting ip reverse list <*name*>
match-interesting ip reverse list <*name*> **in**
match-interesting ip reverse list <*name*> **out**

Syntax Description

list <*name*>	Specifies using an ACL with normal (source, destination) ACL matching logic.
reverse list <*name*>	Specifies using an ACL with reverse (destination, source) ACL matching logic.
in	Optional. Specifies that only incoming traffic is interesting.
out	Optional. Specifies that only outgoing traffic is interesting.

Default Values

By default, no interesting traffic is defined.

Command History

Release 11.1	Command was introduced.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Usage Examples

The following example instructs demand interface **1** to use the access control list **MyACL** when checking for interesting traffic:

(config)**#interface demand 1**
(config-demand 1)**#match-interesting ip list MyACL in**

max-reserved-bandwidth <*value*>

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<*value*>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies **85** percent of the bandwidth on the demand interface 1 be available for use in user-defined queues:

(config)**#interface demand 1**
(config-demand 1)**#max-reserved-bandwidth 85**

ospfv3 <*process id*> **area** <*area id*>

Use the **ospfv3 area** command to add an interface to an Open Shortest Path First version 3 (OSPFv3) process, and to configure the OSPFv3 process on the interface. This command places the interface in the specified area for the specified Internet Protocol version 6 (IPv6) OSPFv3 address family, and optionally defines the instance ID that is used to represent this OSPFv3 process in messages on the interface's link. Use the **no** form of this command to remove the OSPFv3 process from the interface. Variations of this command include:

ospfv3 <*process id*> **area** <*area id*> **ipv6**
ospfv3 <*process id*> **area** <*area id*> **ipv6 instance** <*instance id*>

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join, for the specified address family. The process ID is locally significant to the device, and must be unique among all OSPFv3 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the given OSPFv3 process. Valid range is **0** to **4294967295**.
ipv6	Identifies the OSPFv3 address family as IPv6.
instance <*instance id*>	Optional. Specifies the value to use in the instance ID field of messages sent or received by this OSPFv3 process on the interface's link. Valid range is **0** to **31**.

Default Values

By default, an OSPFv3 process is not configured on an interface. By default, process IDs, area IDs, and instance IDs are not defined.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

When using this command to enable an OSPFv3 process on an interface, keep the following rules in mind:

- The interface must have the address family enabled on the interface. If the address family is not enabled on the interface, the command is rejected and an error is displayed.
- Only interfaces on the default virtual routing and forwarding (VRF) instance support this command. Interfaces on a nondefault VRF will display an error when you attempt to configure OSPFv3 settings.
- The interface and the specified OSPFv3 process (if defined in the global configuration) must be in the same VRF or the command will fail.
- The address family must match that specified for the OSPFv3 process if the process has been defined in the global configuration or the command will fail.
- If the OSPFv3 process identified by the process ID does not exist in the global configuration, it is automatically created, along with the specified address family, and it is assigned to the VRF of which the interface is a member.

- If the specified OSPFv3 process is already at its maximum limit of processes or address families, the command fails.
- If the specified OSPFv3 process already exists in the global configuration, but its configuration does not include an address family, the specified address family is added to the OSPFv3 router configuration.
- A given OSPFv3 process can only have one address family.
- Multiple OSPFv3 instances per address family, per VRF, can be created and can be assigned to a given interface.
- If the interface's VRF changes, all OSPFv3 assignments are removed.
- To change an OSPFv3 process's VRF, the process must first be removed and then recreated. Removing the process removes all OSPFv3 assignments for that process form all interfaces.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To add an interface to the OSPFv3 process **5**, in area **10**, with an instance ID of **10**, enter the command as follows:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 area 10 ipv6 instance 10**

ospfv3 authentication

Use the **ospfv3 authentication** command to authenticate an interface that is performing Internet Protocol version 6 (IPv6) Open Shortest Path First version 3 (OSPFv3) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ospfv3 authentication ipsec spi <*spi*> **md5** <*key*>
ospfv3 authentication ipsec spi <*spi*> **sha1** <*key*>
ospfv3 authentication null

Syntax Description

ipsec	Specifies that IP security (IPsec) authentication is used.
spi <*spi*>	Specifies the security parameter index (SPI). Valid range is **256** to **4294967295**.
md5 <*key*>	Specifies that MD5 authentication is used. Keys are specified in 32 hexadecimal characters.
sha1 <*key*>	Specifies that SHA-1 authentication is used. Keys are specified in 40 hexadecimal characters.
null	Specifies that no OSPFv3 authentication is used.

Default Values

By default, this is set to **null** (meaning no authentication is used).

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example specifies that no OSPFv3 authentication will be used on the interface:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 authentication null**

ospfv3 <*process id*> cost <*cost*>

Use the **ospfv3 cost** command to specify a value that represents the cost of sending an Open Shortest Path First version 3 (OSPFv3) packet over the interface. Use the **no** form of this command to return the cost to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
cost <*cost*>	Specifies the OSPFv3 cost of the interface. This value overrides any automatically computed cost value (default value). Valid range is **1** to **65535**.

Default Values

By default, the OSPFv3 cost of the interface is automatically computed. The automatic cost computation is the reference bandwidth divided by the interface bandwidth. The reference bandwidth is set by the command *auto-cost reference-bandwidth <value> on page 4150*, and defaults to **100** Mbps.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the OSPFv3 cost of the interface as **10**:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 cost 10**

ospfv3 <*process id*> dead-interval <*value*>

Use the **ospfv3 dead-interval** command to specify the maximum interval allowed between Open Shortest Path First version 3 (OSPFv3) Hello packets on the interface. If the maximum interval is exceeded, neighboring devices will assume that the device is down. This value must be the same across all interfaces on a link. Use the **no** form of this command to return the dead interval to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
dead-interval <*value*>	Specifies the maximum number of seconds allowed between OSPFv3 Hello packets. It is recommended that this value be **4** times the Hello packet interval (set with the command *ospfv3 <process id> hello-interval <value> on page 2702*). Valid range is **1** to **65535** seconds.

Default Values

By default, the maximum interval allowed between OSPFv3 Hello packets is set to **40** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To specify the dead interval between OSPFv3 Hello packets on the interface, enter the command as follows:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 dead-interval 100**

ospfv3 encryption

Use the **ospfv3 encryption** command to specify a symmetrical, bidirectional Open Shortest Path First version 3 (OSPFv3) security association (SA) that uses encapsulating security payload (ESP) for encryption and authentication of all OSPFv3 messages that are sent or received on the interface. This command allows you to specify OSPFv3 security at the interface level. Use the **no** form of this command to remove IP security (IPsec) protection of OSPFv3 messages on the interface. Variations of this command include:

ospfv3 encryption ipsec spi <*spi*> **esp** <*encryption type*> <*encryption key*> <*authentication type*> <*authentication key*>
ospfv3 encryption ipsec spi <*spi*> **esp null** <*authentication type*> <*authentication key*>
ospfv3 encryption null

Syntax Description

ipsec	Specifies that IPsec encryption is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by any other IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
esp	Specifies that ESP is used.
null	Specifies that OSPFv3 messages on this interface are not encrypted when used in the **ospfv3 encryption null** format (even when encryption is specified by the OSPFv3 area configuration). When used in the **ospfv3 encryption ipsec spi** <*spi*> **esp null** format, **null** indicates that messages on the interface will not be encrypted, but will be authenticated.
<*encryption type*>	Specifies the type of algorithm used to encrypt OSPFv3 messages. Valid values for encryption are: **3des** uses triple data encryption standard (DES). **aes-cbc** uses advanced encryption standard (AES) with cipher block chaining (CBC). Select from **aes-cbc 128**, **aes-cbc 192**, or **aes-cbc 256**. **des** uses DES.
<*encryption key*>	Specifies the hexadecimal encryption key. The size of the encryption key is determined by the respective encryption algorithm, as follows: **3des** uses a **48** character key size. **aes-cbc 128** uses a **32** character key size. **aes-cbc 192** uses a **48** character key size. **aes-cbc 256** uses a **64** character key size. **des** uses a **16** character key size.
<*authentication type*>	Specifies the algorithm used for authenticating OSPFv3 messages. Valid authentication methods are Message-Digest 5 (**md5**) and Secure-Hash 1 (**sha1**) algorithms.

<authentication key> Specifies the hexadecimal authentication key. The size of the authentication key is determined by the respective authentication algorithm, as follows:

md5 uses a **32** character key size.

sha1 uses a **40** character key size.

Default Values

By default, there is no security for OSPFv3 messages on an interface.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

This commands specifies OSPFv3 security at the interface level. Protection specified with this command overrides any area-level OSPFv3 protection that might apply to the interface.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages with an SPI of **120**, no encryption, and **md5** as the authentication method:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 encryption ipsec spi 120 esp null md5 NeWtStpsswdLoonGpsswDhtThmnWoKEY**

ospfv3 <*process id*> **hello-interval** <*value*>

Use the **ospfv3 hello-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) Hello packets sent on the interface. This value must be the same across all interfaces on the link. Use the **no** form of this command to return the Hello packet interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
hello-interval <*value*>	Specifies the number of seconds allowed between OSPFv3 Hello packets. Valid range is **1** to **65535** seconds.

Default Values

By default, the Hello packet interval for OSPFv3 is **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the interval between OSPFv3 Hello packets on the interface is **20** seconds:

```
(config)#interface demand 1
(config-demand 1)#ospfv3 5 hello-interval 20
```


ospfv3 <*process id*> network

Use the **ospfv3 network** command to specify the network type for Open Shortest Path First version 3 (OSPFv3) enabled interfaces. Use the **no** form of this command to return the interface's network type to the default value. Variations of this command include:

ospfv3 <*process id*> **network broadcast**
ospfv3 <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
broadcast	Specifies that the OSPFv3 network type for the interface is set to broadcast.
point-to-point	Specifies that the OSPFv3 network type for the interface is set to point-to-point.

Default Values

By default, Ethernet interfaces are set to network type broadcast, and point-to-point (PPP), Frame Relay, and loopback interfaces are set to network type point-to-point.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the network interface as point-to-point:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 network point-to-point**

ospfv3 <*process id*> priority <*value*>

Use the **ospfv3 priority** command to specify the Open Shortest Path First version 3 (OSPFv3) priority for the interface. Use the **no** form of this command to return the interface's priority to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
priority <*value*>	Specifies the OSPFv3 priority for the interface. Valid range is **0** to **255**.

Default Values

By default, the OSPFv3 priority of an interface is set to **1**.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

Priority is used in the election of the designated router and backup designated router on multi-access networks. Interfaces connected to multi-access networks (such as Ethernet interfaces) perform an election for a designated and backup designated router. The router interface with the highest OSPFv3 priority on the link becomes the designated router for that link. The interface with the next highest priority becomes the designated backup router. In the event there is a tie, the router interface with the highest router ID takes precedence. A priority value of **0** indicates the router is ineligible to become either the designated or backup designated router.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's OSPFv3 priority value to **6**:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 priority 6**

ospfv3 <*process id*> retransmit-interval <*value*>

Use the **ospfv3 retransmit-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) sent on the interface. Use the **no** form of this command to return the OSPFv3 LSA interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
retransmit-interval <*value*>	Specifies the number of seconds between OSPFv3 LSAs sent on the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA retransmit interval is set to **5** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the LSA retransmit interval is **10** seconds:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 retransmit-interval 10**

ospfv3 <*process id*> shutdown

Use the **ospfv3 shutdown** command to disable an Open Shortest Path First version 3 (OSPFv3) process on the interface. When this command is used, the OSPFv3 commands remain in place, but logically it appears to the interface as though the OSPFv3 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv3 process.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables OSPFv3 process **5** on the interface:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 shutdown**

ospfv3 <*process id*> transmit-delay <*value*>

Use the **ospfv3 transmit-delay** command to specify the estimated time that is required to propagate an Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) on the interface. Use the **no** form of this command to return the transmit delay to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2695*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
transmit-delay <*value*>	Specifies the number of seconds required to send LSAs from the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA transmit delay is set to **1** second.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's LSA transmit delay to **2** seconds:

(config)**#interface demand 1**
(config-demand 1)**#ospfv3 5 transmit-delay 2**

peer default ip address *<ipv4 address>*

Use the **peer default ip address** command to specify the default Internet Protocol version 4 (IPv4) address of the remote end of this interface. Use the **no** form of this command to remove a configured default IPv4 address.

Syntax Description

<ipv4 address>	Specifies the default IPv4 address for the remote end. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there is no assigned peer default IPv4 address.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

This command is useful if the peer does not send the IPv4 address option during Point-to-Point Protocol (PPP) negotiations.

Usage Examples

The following example sets the default peer IPv4 address to **192.22.71.50**:

(config)**#interface demand 1**
(config-demand 1)**#peer default ip address 192.22.71.50**

ppp authentication

Use the **ppp authentication** command to specify the authentication protocol on the Point-to-Point Protocol (PPP) virtual interface that the peer should use to authenticate itself. Use the **no** form of this command to remove configured PPP authentication. Variations of this command include:

ppp authentication chap
ppp authentication pap

Syntax Description

chap	Configures Challenge-Handshake Authentication Protocol (CHAP) authentication on the interface.
pap	Configures Password Authentication Protocol (PAP) authentication on the interface.

Default Values

By default, PPP endpoints have no authentication configured.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Technology Review

CHAP and PAP are two authentication methods that enjoy widespread support. Both methods are included in AOS and are easily configured.

The authentication method set up on the local router can be different from that on the peer. Also, just because one router requires authentication from its peer does not mean it also has to authenticate itself to the peer.

Defining PAP

The PAP is used to verify that the PPP peer is a permitted device by checking a user name and password configured on the peer. The user name and password are both sent unencrypted across the connecting private circuit.

PAP requires a two-way message passing. First, the router that is required to be authenticated (for example, the peer) sends an authentication request with its user name and password to the router requiring authentication (for example, the local router). The local router then looks up the user name and password in the user name database within the PPP interface and, if they match, sends an authentication acknowledge back to the peer.

The PPP user name and password database is separate and distinct from the global user name password database. For PAP and CHAP, use the database under the PPP interface configuration.

Several example scenarios are given below for clarity.

Configuring PAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (host name Local):

Local(config-demand 1)**#ppp authentication pap**
Local(config-demand 1)**#username farend password same**

On the peer (host name Peer):

Peer(config-demand 1)**#ppp pap sent-username farend password same**

The first line of the configuration sets the authentication mode as PAP. This means the peer is required to authenticate itself to the local router via PAP. The second line is the user name and password expected to be sent from the peer. On the peer, the **ppp pap sent-username** command is used to specify the appropriate matching user name and password.

Configuring PAP Example 2: Both routers require the peer to authenticate itself.

On the local router (host name Local):

Local(config-demand 1)**#ppp authentication pap**
Local(config-demand 1)**#username farend password far**
Local(config-demand 1)**#ppp pap sent-username nearend password near**

On the peer (host name Peer):

Peer(config-demand 1)**#ppp authentication pap**
Peer(config-demand 1)**#username nearend password near**
Peer(config-demand 1)**#ppp pap sent-username farend password far**

Now both routers send the authentication request, verify that the user name and password sent match what is expected in the database, and send an authentication acknowledge.

Defining CHAP

The CHAP is a three-way authentication protocol composed of a challenge response and success or failure. The message digest 5 (MD5) protocol is used to protect user names and passwords in the response.

First, the local router (requiring its peer to be authenticated) sends a challenge containing only its own unencrypted user name to the peer. The peer then looks up the user name in the user name database within the PPP interface and, if found, takes the corresponding password and its own host name and sends a response back to the local router. This data is encrypted. The local router verifies that the user name and password are in its own user name database within the PPP interface and, if so, sends a success back to the peer.

The PPP user name and password database is separate and distinct from the global user name password database. For PAP and CHAP, use the database under the PPP interface configuration.

Several example scenarios are given below for clarity.

Configuring CHAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (host name **Local**):

Local(config-demand 1)**#ppp authentication chap**
Local(config-demand 1)**#username Peer password same**

On the peer (host name **Peer**):

Peer(config-demand 1)**#ppp chap password same**

The first line of this configuration sets the authentication mode to CHAP. This means the peer is required to authenticate itself to the local router via CHAP. The second line is the user name and password expected to be sent from the peer. The peer uses its **hostname** and **ppp chap password** commands to send the proper authentication information.

Both ends must have identical passwords.

Configuring CHAP Example 2: Using the ppp chap hostname command as an alternate solution.

On the local router (host name **Local**):

Local(config-demand 1)**#ppp authentication chap**
Local(config-demand 1)**#username farend password same**

On the peer (host name **Peer**):

Peer(config-demand 1)**#ppp chap hostname farend**
Peer(config-demand 1)**#ppp chap password same**

Notice the local router is expecting user name **farend** even though the peer router's host name is **Peer**. Therefore, the peer router can use the **ppp chap hostname** command to send the correct name in the challenge.

Both ends must have identical passwords.

Configuring CHAP Example 3: Both routers require each other to authenticate themselves using the same shared password.

On the local router (host name **Local**):

Local(config-demand 1)**#ppp authentication chap**
Local(config-demand 1)**#username Peer password same**

On the peer (host name **Peer**):

Peer(config-demand 1)**#ppp authentication chap**
Peer(config-demand 1)**#username Local password same**

This is basically identical to Example 1 except that both routers will now challenge each other and respond.

Both ends must have identical passwords.

Configuring CHAP Example 4: Both routers require each other to authenticate themselves using two separate shared passwords.

On the local router (host name **Local**):

Local(config-demand 1)**#ppp authentication chap**
Local(config-demand 1)**#username Peer password far**
Local(config-demand 1)**#ppp chap password near**

On the peer (host name **Peer**):

Peer(config-demand 1)**#ppp authentication chap**
Peer(config-demand 1)**#username Local password near**
Peer(config-demand 1)**#ppp chap password far**

This is basically identical to Example 3, except that there are two separate shared passwords.

Notice this example has both ends using different sets of passwords.

Configuring CHAP Example 5: Using the ppp chap hostname command as an alternate solution.

On the local router (host name **Local**):

Local(config-demand 1)**#ppp authentication chap**
Local(config-demand 1)**#username farend password far**
Local(config-demand 1)**#ppp chap hostname nearend**
Local(config-demand 1)**#ppp chap password near**

On the peer (host name **Peer**):

Peer(config-demand 1)**#ppp authentication chap**
Peer(config-demand 1)**#username nearend password near**
Peer(config-demand 1)**#ppp chap hostname farend**
Peer(config-demand 1)**#ppp chap password far**

Notice the local router is expecting user name **farend** even though the peer router's host name is **Peer**. Therefore, the peer router can use the **ppp chap hostname** command to send the correct name on the challenge.

Notice this example has both ends using different sets of passwords.

ppp bcp tagged-frame

Use the **ppp bcp tagged-frame** command to allow negotiation of IEEE 802.1Q-tagged packets over Bridging Control Protocol (BCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example configures the interface to negotiate tagged frames over **bcp**:

(config)**#interface demand 1**
(config-demand 1)**#ppp bcp tagged-frame**

ppp chap hostname *<name>*

Use the **ppp chap hostname** command to configure an alternate host name for Challenge-Handshake Authentication Protocol (CHAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured host name. For more information on Password Authentication Protocol (PAP) and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication on page 2709*.

Syntax Description

<name>	Specifies a host name using an alphanumeric string up to 80 characters in length.

Default Values

By default, there are no configured PPP CHAP host names.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Usage Examples

The following example specifies a PPP CHAP host name of **my_host**:

(config)**#interface demand 1**
(config-demand 1)**#ppp chap hostname my_host**

ppp chap password *<password>*

Use the **ppp chap password** command to configure an alternate password when the peer requires Challenge-Handshake Authentication Protocol (CHAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured password. For more information on Password Authentication Protocol (PAP) and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication on page 2709*.

Syntax Description

<password>	Specifies a password using an alphanumeric string up to 80 characters in length.

Default Values

By default, there is no defined PPP CHAP password.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Usage Examples

The following example specifies a PPP CHAP password of **my_password**:

(config)**#interface demand 1**
(config-demand 1)**#ppp chap password my_password**

ppp multilink

Use the **ppp multilink** command to enable Multilink Point-to-Point Protocol (MLPPP) operation on an existing Point-to-Point Protocol (PPP) interface. Use the **no** form of this command to disable this feature. Variations of this command include:

ppp multilink
ppp multilink fragmentation
ppp multilink interleave
ppp multilink maximum <*number*>

Syntax Description

fragmentation	Enables multilink fragmentation operation.
interleave	Enables multilink interleave operation.
maximum <*number*>	Specifies the maximum number of links allowed in a PPP multilink bundle.

Default Values

By default, MLPPP is disabled.

Command History

Release 7.1	Command was introduced.
Release 7.2	Fragmentation and interleave operation were added.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

When enabled, this interface is capable of the following:

- Combining multiple physical links into one logical link.
- Receiving upper layer protocol data units (PDUs), fragmenting and transmitting over the physical links.
- Receiving fragments over the physical links and reassembling them into PDUs.

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as being high priority. Delivery in order is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

The multilink bundle will remain active with a minimum of one physical link. Physical links may be dynamically added or removed from the multilink bundle with minor interruption to traffic flow.

Usage Examples

The following example enables MLPPP:

(config)**#interface demand 1**
(config-demand 1)**#ppp multilink**

ppp mtu *<size>*

Use the **ppp mtu** command to configure the Point-to-Point Protocol (PPP) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Configures the window size for transmitted packets. The valid range is **64** to **2100** bytes.

Default Values

By default, the PPP MTU on an interface is set to **1500** bytes.

Command History

Release 17.9	Command was introduced.

Usage Examples

The following example specifies a PPP MTU of **1200** on the virtual demand interface:

(config)**#interface demand 1**
(config-demand 1)**#ppp mtu 1200**

ppp pap sent-username <*username*> password <*password*>

Use the **ppp pap sent-username password** command to configure a user name and password when the peer requires Password Authentication Protocol (PAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured password. For more information on PAP and Challenge-Handshake Authentication Protocol (CHAP) functionality, refer to the *Technology Review* section for the command *ppp authentication on page 2709*.

Syntax Description

<username>	Specifies a user name by alphanumeric string up to 80 characters in length (the user name is case sensitive).
<password>	Specifies a password by alphanumeric string up to 80 characters in length (the password is case sensitive).

Default Values

By default, there is no defined **ppp pap sent-username** and **password**.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Usage Examples

The following example specifies a PPP PAP sent-user name of **local** and a password of **my_password**:

(config)**#interface demand 1**
(config-demand 1)**#ppp pap sent-username local password my_password**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in <*name*>
qos-policy out <*name*>

Syntax Description

<*name*>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the **in** parameter.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the demand 1 interface:

(config)**#interface demand 1**
(config-demand 1)**#qos-policy out VOICEMAP**

resource pool *<name>*

Use the **resource pool** command to associate a resource pool with the demand interface. No more than one resource pool may be associated with an interface. Refer to *resource pool-member <name> on page 2101* for more information. Use the **no** form of this command to restore the default value.

Syntax Description

<name>	Specifies the resource pool that this interface will use to originate/answer demand connections.

Default Values

By default, no resource pool is associated with this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example associates the resource pool named **Pool1** with demand interface **1**:

(config)**#interface demand 1**
(config-demand 1)**#resource pool Pool1**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the virtual demand interface:

(config)**#interface demand 1**
(config-demand 1)**#rtp quality-monitoring**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.2	Command was expanded to the cellular interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the virtual demand interface:

(config)**#interface demand 1**
(config-demand 1)**#no snmp trap link-status**

username *<username>* **password** *<password>*

Use the **username password** command to configure the user name and password of the peer to use for demand authentication. Use the **no** form of this command to remove a configured user name and password.

Syntax Description

<username>	Specifies a user name by alphanumerical string up to 30 characters in length (the user name is case sensitive).
<password>	Specifies a password by alphanumerical string up to 30 characters in length (the password is case sensitive).

Default Values

By default, there is no established user name and password.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

Password Authentication Protocol (PAP) uses this entry to check received information from the peer. Challenge-Handshake Authentication Protocol (CHAP) uses this entry to check the received peer host name and a common password.

Usage Examples

The following example creates a user name of **Adtran** with password **Adtran** for the demand link labeled **5**:

(config)**#interface demand 5**
(config-demand 5)**#username Adtran password Adtran**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the virtual demand interface to the VRF instance named **RED**:

(config)**#interface demand 1**
(config-demand 1)**#vrf forwarding RED**

FRAME RELAY INTERFACE COMMAND SET

To create a virtual Frame Relay interface and activate the Frame Relay Interface Configuration mode, enter the **interface frame-relay** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface frame-relay 1
(config-fr 1)#
```

By default, Frame Relay interfaces are created as point-to-point links. This default setting cannot be altered. The following command creates the exact same interface as that mentioned above:

```
>enable
#configure terminal
(config)#interface frame-relay 1 point-to-point
(config-fr 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bandwidth <value> on page 2728
encapsulation frame-relay ietf on page 2729
fair-queue on page 2730
frame-relay commands begin on page 2731
hold-queue <value> out on page 2742
max-reserved-bandwidth <value> on page 2743
qos-policy on page 2744
snmp trap on page 2746
snmp trap link-status on page 2747

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.

Functional Notes

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 2743*) to adjust the bandwidth appropriately for QoS configurations.

Usage Examples

The following example sets bandwidth of the Frame Relay interface to 10 Mbps:

(config)**#interface frame-relay 1**
(config-fr 1)**#bandwidth 10000**

encapsulation frame-relay ietf

Use the **encapsulation frame-relay ietf** command to configure the encapsulation on a virtual Frame Relay interface as IETF (RFC 1490). Currently, this is the only encapsulation setting. Settings for this option must match the far-end router's settings in order for the Frame Relay interface to become active.

Syntax Description

No subcommands.

Default Values

By default, all Frame Relay interfaces use IETF encapsulation.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the endpoint for IETF encapsulation:

(config)**#interface frame-relay 1**
(config-fr 1)**#encapsulation frame-relay ietf**

fair-queue

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable first in, first out (FIFO) queueing for an interface. Variations of this command include:

fair-queue
fair-queue <*value*>

WFQ must be enabled on an interface to use priority queuing. By default, WFQ is enabled for all interfaces with maximum bandwidth speeds equivalent to T1/E1 and below.

Syntax Description

<*value*>	Optional. Specifies the maximum number of packets that can be present in each conversation subqueue. Packets received for a conversation after this limit is reached are discarded. Range is **16** to **512** packets.

Default Values

By default, **fair-queue** is enabled with a threshold of 64 packets.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables WFQ on the interface with a threshold set at 100 packets:

(config)**#interface frame-relay 1**
(config-fr 1)**#fair-queue 100**

frame-relay intf-type

Use the **frame-relay intf-type** command to define the Frame Relay signaling role needed for the endpoint. Use the **no** form of this command to return to the default value. Variations of this command include:

frame-relay intf-type dce
frame-relay intf-type dte
frame-relay intf-type nni

Syntax Description

dce	Specifies data communication equipment (DCE) or network-signaling role. Use this interface type when you need the unit to emulate the frame switch.
dte	Specifies data terminal equipment (DTE) or user-signaling role. Use this interface type when connecting to a Frame Relay switch (or piece of equipment emulating a frame switch).
nni	Configures the interface to support both network and user signaling (DTE or DCE) when necessary.

Default Values

By default, **frame-relay intf-type** is set to **dte**.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the Frame Relay endpoint for DCE signaling:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay intf-type dce**

frame-relay lmi-n391dte <*value*>

Use the **frame-relay lmi-n391dte** command to set the N391 full status polling counter for the data terminal equipment (DTE) endpoint. Typical applications should leave the default value for this timer. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Sets the poll counter value. Valid range is **1** to **255**.

Default Values

By default, the polling counter for the DTE endpoint is set to six polls.

Command History

Release 1.1	Command was introduced.

Functional Notes

The N391 counter determines how many link integrity polls occur in between full status polls. The number of link integrity polls between full status polls is n - 1, where n represents the full status poll. n can be set to any number between 1 and 255, but the default is used for most applications.

Usage Examples

The following example sets the N391 counter for three polls:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-n391dte 3**

frame-relay lmi-n392dce <*value*>

Use the **frame-relay lmi-n392dce** command to set the N392 error threshold for the data communication equipment (DCE) endpoint. Typical applications should leave the default value for this setting. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Sets the error threshold value. Valid range is **1** to **10** errors.

Default Values

By default, the error threshold for the DCE endpoint is set to three errors.

Command History

Release 1.1	Command was introduced.

Functional Notes

If the error threshold is met, the signaling state status is changed to down, indicating a service-affecting condition. This condition is cleared once N393 consecutive error-free events are received. N392 defines the number of errors required in a given event window, while N393 defines the number of polling events in each window.

For example:

If N392 = 3 and N393 = 4, then if three errors occur within any four events, the interface is determined inactive.

Usage Examples

The following example sets the N392 threshold for 5 seconds:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-n392dce 5**

frame-relay lmi-n392dte <*value*>

Use the **frame-relay lmi-n392dte** command to set the N392 error threshold for the data terminal equipment (DTE) endpoint. Typical applications should leave the default value for this setting. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Sets the error threshold value. Valid range is **1** to **10** errors.

Default Values

By default, the error threshold for the DTE endpoint is set to three errors.

Command History

Release 1.1	Command was introduced.

Functional Notes

If the error threshold is met, the signaling state status is changed to down, indicating a service-affecting condition. This condition is cleared once N393 consecutive error-free events are received. N392 defines the number of errors required in a given event window, while N393 defines the number of polling events in each window.

For example:

If N392 = 3 and N393 = 4, then if three errors occur within any four events, the interface is determined inactive.

Usage Examples

The following example sets the N392 threshold for five errors:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-n392dte 5**

frame-relay lmi-n393dce <*value*>

Use the **frame-relay lmi-n393dce** command to set the N393 local management interface (LMI) monitored event counter for the data communication equipment (DCE) endpoint. Typical applications should leave the default value for this counter. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Sets the event counter value. Valid range is **1** to **10** events.

Default Values

By default, the LMI monitored event counter for the DCE endpoint is set to four events.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sets the N393 threshold for five events:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-n393dce 5**

frame-relay lmi-n393dte <*value*>

Use the **frame-relay lmi-n393dte** command to set the N393 local management interface (LMI) monitored event counter for the data terminal equipment (DTE) endpoint. Typical applications should leave the default value for this counter. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Sets the event counter value. Valid range is **1** to **10** events.

Default Values

By default, the LMI monitored event counter for the DTE endpoint is set to four events.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sets the N393 threshold for five events:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-n393dte 5**

frame-relay lmi-t391dte <*value*>

Use the **frame-relay lmi-t391dte** command to set the T391 signal polling timer for the data terminal equipment (DTE) endpoint. Typical applications should leave the default value for this timer. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Sets the signal polling timer value in seconds. Valid range is **5** to **30** seconds.

Default Values

By default, the signal polling timer for the DTE endpoint is set to **10** seconds.

Command History

Release 1.1	Command was introduced.

Functional Notes

The T391 timer sets the time (in seconds) between polls to the Frame Relay network.

Usage Examples

The following example sets the T391 timer for 15 seconds:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-t391dte 15**

frame-relay lmi-t392dce <*value*>

Use the **frame-relay lmi-t392dce** command to set the T392 polling verification timer for the data communication equipment (DCE) endpoint. Typical applications should leave the default value for this timer. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Sets the polling verification timer value in seconds. Valid range is **5** to **30** seconds.

Default Values

By default, the polling verification timer for the DCE endpoint is set to **10** seconds.

Command History

Release 1.1	Command was introduced.

Functional Notes

The T392 sets the timeout (in seconds) between polling intervals. This parameter needs to be a few seconds longer than the T391 setting of the attached Frame Relay device.

Usage Examples

The following example sets the T392 timer for 15 seconds:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-t392dce 15**

frame-relay lmi-type

Use the **frame-relay lmi-type** command to define the Frame Relay signaling (local management interface (LMI)) type. Use the **no** form of this command to return to the default value. Variations of this command include:

frame-relay lmi-type ansi
frame-relay lmi-type auto
frame-relay lmi-type cisco
frame-relay lmi-type none
frame-relay lmi-type q933a

Syntax Description

ansi	Specifies Annex D signaling method.
auto	Automatically determines signaling type by messages received on the frame circuit.
cisco	Specifies Group of 4 signaling method.
none	Turns off signaling on the endpoint. This is used for dial-backup connections to Adtran IQ and Express Series products.
q933a	Specifies Annex A signaling method.

Default Values

By default, the Frame Relay signaling type is set to **ansi**.

Command History

Release 1.1	Command was introduced.
Release 2.1	Added signaling type **none** to provide support for dial-backup to Adtran IQ and Express Series products.

Usage Examples

The following example sets the signaling method for the endpoint to **cisco**:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay lmi-type cisco**

frame-relay multilink

Use the **frame-relay multilink** command to enable the Frame Relay multilink interface. When the **no** form of this command is issued, all configuration options associated with this command and cross connects made to this interface are removed. Variations of this command include:

frame-relay multilink
frame-relay multilink ack <*value*>
frame-relay multilink bandwidth-class [A | B]
frame-relay multilink bandwidth-class C <*threshold*>
frame-relay multilink bid <*string*>
frame-relay multilink hello <*value*>
frame-relay multilink retry <*number*>

Syntax Description

ack <*value*>	Optional. Specifies a wait for acknowledgement time (in seconds) for every bundle link in the bundle. Range is **1** to **180** seconds.
bandwidth-class	Optional. Specifies the class of operation, placing a minimum limit on the acceptable amount of bandwidth required for a bundle to be up.
[A | B]	Optional. Specifies the class of operation. Class A A single active link is sufficient for the bundle to be up. Class B All defined bundle links must be active for the bundle to be up.
C <*threshold*>	Optional. Specifies the minimum number of active bundle links required for a Class C bundle to be in the up state. This option will not be available unless Class C is specified. Range is **1** to **65535** links.
bid <*string*>	Optional. Specifies a bundle ID (up to 48 characters) for the multilink bundle. All hello messages sent on links belonging to the multilink bundle contain the bundle ID. By default, AOS creates a generic bundle ID for each configured multilink bundle using the following: **MFR** <*interface number*> where the interface number corresponds to the interface number of the Frame Relay interface. For example, if multilink is enabled on Frame Relay interface 1, by default the bundle ID is **MFR1**. Changing the bundle ID causes the multilink connection to go down for renegotiation.
hello <*value*>	Optional. Specifies the time (in seconds) between hello messages for every bundle link in the bundle. Range is **1** to **180** seconds.
retry <*number*>	Optional. Specifies the number of times a bundle link will retransmit a message while waiting for acknowledgement. Range is **1** to **5** times.

Default Values

The default **ack** value is 4 seconds. The default **hello** value is 10 seconds. The default <*class*> value is A. The default **retry** value is 2.

Command History

Release 9.1	Command was introduced.

Functional Notes

This command is different from **ppp multilink**. In **ppp multilink**, if multiple cross connects are configured for the Point-to-Point Protocol (PPP) interface without multilink PPP being enabled, the first link to bring up Link Control Protocol (LCP) will be the only link actually cross connected. In Frame Relay multilink, since there is no protocol corresponding to LCP, all cross connects will be removed and the user will be free to re-issue any cross connect.

Usage Examples

The following example enables the Frame Relay multilink interface and sets the time between **hello** messages to **45** seconds:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay multilink hello 45**

The following example specifies Class B operation:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay multilink bandwidth-class B**

The following example specifies Class C operation with a threshold of **5**:

(config)**#interface frame-relay 1**
(config-fr 1)**#frame-relay multilink bandwidth-class C 5**

hold-queue <*value*> out

Use the **hold-queue out** command to change the overall size of an interface's wide area network (WAN) output queue. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the total number of packets the output queue can contain before packets are dropped. Range is **16** to **1000** packets.

Default Values

The default queue size for weighted fair queuing (WFQ) is 400. The default queue size for Point-to-Point Protocol (PPP) first in, first out (FIFO) and Frame Relay round robin is 200.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the overall output queue size to 700:

(config)**#interface frame-relay 1**
(config-fr 1)**#hold-queue 700 out**

max-reserved-bandwidth *<value>*

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<value>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies **85** percent of the bandwidth on the Frame Relay 1 interface to be available for use in user-defined queues:

(config)**#interface frame-relay 1**
(config-fr 1)**#max-reserved-bandwidth 85**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing (WFQ).
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the Frame Relay interface:

(config)**#interface frame-relay 1**
(config-fr 1)**#qos-policy out VOICEMAP**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP on the virtual Frame Relay interface:

(config)**#interface frame-relay 1**
(config-fr 1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the Frame Relay interface:

(config)**#interface frame-relay 1**
(config-fr 1)**#no snmp trap link-status**

FRAME RELAY SUBINTERFACE COMMAND SET

To create a virtual Frame Relay subinterface and activate the Frame Relay Subinterface Configuration mode, enter the **interface frame-relay** command (and specify a subinterface) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminalF
(config)#interface frame-relay 1.16
(config-fr 1.16)#
```

By default, Frame Relay subinterfaces are created as point-to-point links. This default setting cannot be altered. The following command creates the exact same interface as that mentioned above:

```
>enable
#configure terminal
(config)#interface frame-relay 1.16 point-to-point
(config-fr 1.16)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bandwidth <value> on page 2750
bridge-group <number> on page 2751
bridge-group <number> vlan-transparent on page 2752
dial-backup commands begin on page 2753
dynamic-dns on page 2770
frame-relay commands begin on page 2772
ip commands begin on page 2776
ipv6 commands begin on page 2821
lldp receive on page 2858
lldp send on page 2859
media-gateway ip on page 2861

media-gateway ipv6 on page 2863
ospfv3 commands begin on page 2865
rtp quality-monitoring on page 2878
snmp trap on page 2879
snmp trap link-status on page 2880
spanning-tree commands begin on page 2881
vrf forwarding <name> on page 2887

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view the default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.

Functional Notes

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface.

Usage Examples

The following example sets bandwidth of the Frame Relay interface to 10 Mbps:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#bandwidth 10000**

bridge-group *<number>*

Use the **bridge-group** command to assign an interface to the specified bridge group. This command is supported on all Ethernet interfaces, Point-to-Point Protocol (PPP) virtual interfaces, and Frame Relay virtual subinterfaces. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<number>	Specifies the bridge group number. Range is **1** to **255**.

Default Values

By default, there are no configured bridge groups.

Command History

Release 1.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (Ethernet to T1 bridge, Ethernet to Frame Relay subinterface).

Usage Examples

The following example assigns the Frame Relay subinterface labeled 1.16 to bridge group 1:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#bridge-group 1**

bridge-group <*number*> vlan-transparent

Use the **bridge-group vlan-transparent** command to prevent an interface from removing the virtual local area network (VLAN) tag. Use the **no** form of this command to allow the interface to remove the VLAN tag from the packet.

*The **bridge-group vlan-transparent** command is not a global command. The command must be applied on all interfaces of the bridge group.*

Syntax Description

<number>	Specifies the bridge group number. Valid range is **1** to **255**.

Default Values

By default, VLAN tags are removed from the data.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the high level data link control (HDLC) interface and Frame Relay subinterface.

Usage Examples

The following example removes the VLAN tags from the packets on the Frame Relay subinterface labeled 1.16:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#bridge-group 1 vlan-transparent**

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the interface to automatically attempt a dial backup upon failure. Use the **no** form of this command to disable this feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial backup upon a failure.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables automatic dial backup on the endpoint:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup auto-backup**

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial-backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures AOS to automatically restore the primary connection when the failure condition clears:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup auto-restore**

dial-backup backup-delay *<value>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

<value>	Specifies the delay period (in seconds) a failure must be active before AOS will enter backup operation on the interface. Range is **10** to **86400** seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to 10 seconds.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures AOS to wait **60** seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup backup-delay 60**

dial-backup call-mode

Use the **dial-backup call-mode** command to specify whether the configured backup interface answers or originates (or a combination of both) backup calls. Use the **no** form of this command to return to the default value. Variations of this command include:

dial-backup call-mode answer
dial-backup call-mode answer-always
dial-backup call-mode originate
dial-backup call-mode originate-answer
dial-backup call-mode originate-answer-always

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer**.

Command History

Release 1.1	Command was introduced.

Functional Notes

The majority of the configuration for AOS dial-backup implementation is configured via the dial-backup Point-to-Point Protocol (PPP) interface configuration commands. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname “Remote3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.1.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
 coding b8zs
 framing esf
```



```
 clock source line
 tdm-group 1 timeslots 1-24
 no shutdown
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.16 point-to-point
 frame-relay interface-dlci 16
 ip address 10.1.1.2 255.255.255.252
 dial-backup call-mode originate
 dial-backup number 5551111 analog ppp1
 dial-backup number 5552222 analog ppp1
no shutdown
!
interface ppp 1
 ip address 172.22.56.1 255.255.255.252
 ppp authentication chap
 username remoterouter password remotepass
 ppp chap hostname localrouter
 ppp chap password adtran
 no shutdown
!
ip route 192.168.2.0 255.255.255.0 172.22.56.2 255.255.255.252
!
line telnet 0 4
 password password
```

Sample configuration for central router (dialing in)

```
hostname “Central3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.100.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
 coding b8zs
 framing esf
 clock source line
 tdm-group 1 timeslots 1-24
 no shutdown
```



```
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.100 point-to-point
 frame-relay interface-dlci 100
 ip address 10.1.1.1 255.255.255.252
 dial-backup call-mode answer
 dial-backup number 555-8888 analog ppp 1
!
interface ppp 1
 ip address 172.22.56.2 255.255.255.252
 ppp authentication chap
 username localrouter password adtran
 ppp chap hostname remoterouter
 ppp chap password remotepass
 no shutdown
!
ip route 192.168.1.0 255.255.255.0 172.22.56.1 255.255.255.252

line telnet 0 4
 password password
```

Usage Examples

The following example configures AOS to generate backup calls for this endpoint using an analog modem interface (to phone number 555 1111), but never answer calls and specifies **ppp 1** as the backup interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup call-mode originate
(config-fr 1.16)#dial-backup number 555 1111 analog ppp 1
```

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial backup, where in the configuration AOS accesses specific routing information, etc.):

Dialing Out

1. AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number <number> on page 2763*).
3. When placing the call, AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, AOS places a call to the second number (if a second number is configured). The second number to be dialed references a separate PPP interface.

Dialing In

1. AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from caller ID, the call is terminated.

dial-backup connect-timeout <*value*>

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

<*value*>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call. Valid range is **10** to **300** seconds.

Default Values

By default, the **dial-backup connect-timeout** period is set to 60 seconds.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures AOS to wait **120** seconds before retrying a failed dial-backup call:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup connect-timeout 120**

dial-backup force

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*. Variations of this command include:

dial-backup force backup
dial-backup force primary

Syntax Description

backup	Force backup regardless of primary link state.
primary	Force primary link regardless of its state.

Default Values

By default, this feature is disabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures AOS to force this interface into dial backup:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup force backup**

dial-backup maximum-retry <*value*>

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

<*value*>	Selects the number of call retries that will be made after a link failure. Valid range is **0** to **15** attempts. Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to 0 attempts.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures AOS to retry a dial-backup call four times before considering backup operation not available:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup maximum-retry 4**

dial-backup number <*number*>

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. Use the **no** form of this command to disable this feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2756*. Variations of this command include:

dial-backup number <*number*> **analog ppp** <*interface*>
dial-backup number <*number*> **digital-56k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>
dial-backup number <*number*> **digital-64k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>

Syntax Description

<*number*>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates the number connects to an analog modem.
digital-56k	Indicates the number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates the number belongs to a digital 64 kbps per DS0 connection.
<*isdn min chan*>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
<*isdn max chan*>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
ppp <*interface*>	Specifies the Point-to-Point Protocol (PPP) interface to use as the backup for this interface (for example, **ppp 1**).

Default Values

By default, there are no configured dial-backup numbers.

Command History

Release 1.1	Command was introduced.
Release 17.2	Command was expanded to include the cellular connections.
Release 17.3	Cellular connections were removed from this command.

Usage Examples

The following example configures AOS to dial **704-555-1212** (digital 64 kbps connection) to initiate dial-backup operation for this endpoint using the configured **ppp 1** backup interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup number 7045551212 digital-64k 1 1 ppp 1**

dial-backup priority <*value*>

Use the **dial-backup priority** command to select the backup priority for this interface. This command allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

<*value*>	Sets the relative priority of this link. Valid range is **0** to **100**. A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to 50.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example assigns the highest priority to this endpoint:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup priority 100**

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

No subcommands.

Default Values

By default, AOS does not randomize the dial-backup call timers.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures AOS to randomize the dial-backup timers associated with this endpoint:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup randomize-timers**

dial-backup redial-delay <*value*>

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

<*value*>	Specifies the delay in seconds between attempting to redial a failed backup attempt. Range is **10** to **3600** seconds.

Default Values

By default, **dial-backup redial-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures a redial delay of **25** seconds on this endpoint:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup redial-delay 25**

dial-backup restore-delay *<value>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is bouncing in and out of alarm. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

<value>	Specifies the number of seconds AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range is **10** to **86400** seconds.

Default Values

By default, **dial-backup restore-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures AOS to wait **30** seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup restore-delay 30**

dial-backup schedule

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial backup (as specified). For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*. Variations of this command include:

dial-backup schedule day <*name*>
dial-backup schedule enable-time <*value*>
dial-backup schedule disable-time <*value*>

Syntax Description

day <*name*>	Sets the days to allow backup. Valid range is Monday through Sunday.
enable-time <*value*>	Sets the time of day to enable backup. Time is entered in a 24-hour format (00:00).
disable-time <*value*>	Sets the time of day to disable backup. Time is entered in a 24-hour format (00:00).

Default Values

By default, dial backup is enabled for all days and times if the **dial-backup auto-backup** command has been issued and the dial-backup schedule has not been entered.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables dial backup Monday through Friday 8:00 a.m. to 7:00 p.m.:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup schedule enable-time 08:00**
(config-fr 1.16)**#dial-backup schedule disable-time 19:00**
(config-fr 1.16)**#no dial-backup schedule day Saturday**
(config-fr 1.16)**#no dial-backup schedule day Sunday**

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2756*.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are disabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example deactivates the configured dial-backup interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dial-backup shutdown**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#dynamic-dns dyndns-custom host user pass**

frame-relay bc *<value>*

Use the **frame-relay bc** command to set the b_c (committed burst) value for a Frame Relay sublink. The value is in bits. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the committed burst value (in bits) for the sublink.

Default Values

By default, the committed burst value is set to **0** (no limit).

Command History

Release 4.1	Command was introduced.

Functional Notes

The time interval is always one second, so this can also be considered bits per second. Shaping is performed on a sliding one-second window to make maximum use of configured bandwidth. Note that when both b_c and b_e are nonzero, shaping is performed on the virtual circuit. The circuit is limited to the sum of b_c and b_e , and it is recommended that the sum always be greater than 8000.

Usage Examples

The following example configures the Frame Relay sublink with a committed burst value of 128,000 bits:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#frame-relay bc 128000**

frame-relay be *<value>*

Use the **frame-relay be** command to set the b_e (excessive burst) value for a Frame Relay sublink. The value is in bits. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the excessive burst value (in bits) for the sublink.

Default Values

By default, the excessive burst value is set to **0** (no limit).

Command History

Release 4.1	Command was introduced.

Functional Notes

The time interval is always one second, so this can also be considered bits per second. Shaping is performed on a sliding one-second window to make maximum use of configured bandwidth. Note that when both b_c and b_e are nonzero, shaping is performed on the virtual circuit. The circuit is limited to the sum of b_c and b_e, and it is recommended that the sum always be greater than 8000.

Usage Examples

The following example configures the Frame Relay sublink with an excessive burst value of 64,000 bits:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#frame-relay be 64000**

frame-relay fragment <*value*>

Use the **frame-relay fragment** command to set the FRF.12 fragmentation threshold. Use the **no** form of this command to erase the configured threshold.

Syntax Description

<*value*>	Specifies the fragmentation threshold. Valid fragmentation thresholds are greater than or equal to 64 and less than or equal to 1600.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Functional Notes

For Frame Relay fragmentation to take effect, rate-limiting must be enabled by setting the committed burst rate and excessive burst rate. Refer to *frame-relay bc <value> on page 2772* and *frame-relay be <value> on page 2773* for more information.

Usage Examples

The following example enables FRF.12 fragmentation on a sublink:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#frame-relay bc 64000**
(config-fr 1.16)**#frame-relay be 16**
(config-fr 1.16)**#frame-relay fragment 100**

The following example disables FRF.12 fragmentation on a sublink:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#no frame-relay fragment**

frame-relay interface-dlci <*value*>

Use the **frame-relay interface-dlci** command to configure the data link connection identifier (DLCI) for the Frame Relay subinterface. This setting should match the DLCI supplied by your Frame Relay service provider. Use the **no** form of this command to remove the configured DLCI.

Syntax Description

<*value*>	Specifies numeric value of the DLCI supplied by your provider.

Default Values

By default, the DLCI is populated with the subinterface identifier. For example, if configuring the virtual Frame Relay subinterface labeled **fr 1.20**, the default DLCI is **20**.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures a DLCI of **72** for this Frame Relay endpoint:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#frame-relay interface-dlci 72**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to create an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Specifies the IPv4 ACL name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic into the Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#int frame-relay 1.16**
(config-fr 1.16)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip access-policy PRIVATE**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii <*string*> **| hex** <*value*>**] [client-id [**<*interface*> **|** <*identifier*>**]] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp client-id [<*interface*> **|** <*identifier*>**] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp hostname *"*<*string*>*"* **[no-default-route | no-domain-name | no-nameservers] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track <*name*>**] [**<*administrative distance*>**]**
ip address dhcp track <*name*> **[**<*administrative distance*>**]**

Syntax Description

<*administrative distance*>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii <*string*>	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex <*value*>	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<*interface*>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<*identifier*>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the <*identifier*> option.
hostname <*"string"*>	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

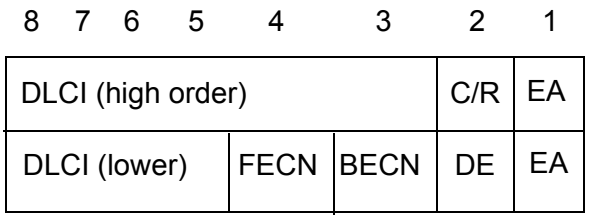
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *“<string>”* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip address dhcp hostname “adtran” no-default-route no-domain-name no-nameservers 5**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 255.255.255.252**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip address 192.22.72.101 255.255.255.252 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

> NOTE *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.*

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

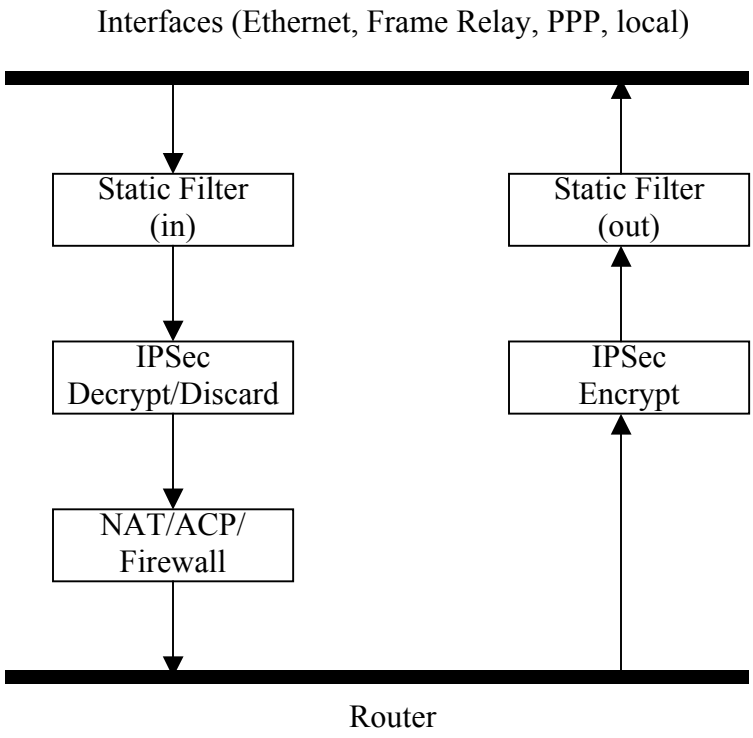
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip crypto map MyMap**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).

Usage Examples

The following example releases the IPv4 DHCP address for the virtual interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip dhcp release**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **frame-relay 1.16**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 4 (IPv4) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries to be cleared from this IPv4 interface.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.4.0	Maximum number of stored entries was expanded to **500000** and RapidRoute is now enabled by default.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv4 interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#no ip ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on a **Frame Relay** interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper-address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (**255.255.255.255**) or a subnet broadcast (for example, **192.33.4.251** for the **192.33.4.248 /30** subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#interface frame-relay 1.16**
(config)**#ip forward-protocol udp domain**
(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip mcast-stub downstream**

ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*address*> command (refer to *ip igmp on page 2795*) to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include the Frame Relay subinterfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 2797*, and *ip mcast-stub upstream on page 2800* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 2797* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the Frame Relay interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip ospf 1 network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the Frame Relay subinterface every **3600** seconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to **300** seconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation delay to **300** milliseconds on the Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP **version 1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that will override the **version** (in the Router RIP) configuration.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures a Frame Relay subinterface to accept only RIP version 2 packets:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP **version 1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip send version** to specify a RIP version that will override the **version** (in the Router RIP) configuration.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures a Frame Relay subinterface to transmit only RIP version 2 packets:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable Internet Protocol version 4 (IPv4) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Fast switching allows an IPv4 interface to provide optimum performance when processing IPv4 traffic.

Usage Examples

The following example enables IPv4 fast switching on the Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Frame Relay Subinterface Configuration mode configures the Frame Relay subinterface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the Frame Relay interface (labeled **frame-relay 1.16**) to use the IP address assigned to the Ethernet interface (**eth 0/1**):

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip unnumbered eth 0/1**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through a Frame Relay subinterface and matches the URL filter named **MyFilter**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on an interface. Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the interface.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the interface to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the interface.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an interface when other unicast IPv6 addresses are not needed on the interface. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the interface.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6**

ipv6 access-group *<ipv6 acl name>*

Use the **ipv6 access-group** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to be used for IPv6 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ipv6 access-group <*ipv6 acl name*> **in**
ipv6 access-group <*ipv6 acl name*> **out**

Syntax Description

<ipv6 acl name>	Applies the named IPv6 ACL to the interface.
in	Enables access control on IPv6 packets received on the specified interface.
out	Enables access control on IPv6 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 18.1	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Only one IPv6 ACL can be applied in each traffic direction.

Unlike in IPv4, IPv6 traffic filters include an implicit **permit** for neighbor solicitation and advertisement packets in an ACL before the traditional implicit **deny** at the end of the ACL. This prevents blocking of address resolution and unreachability detection, although this can be overridden by entering explicit **deny** commands in the IPv6 ACL.

Usage Examples

The following example applies the IPv6 ACL **Privatev6** to incoming IPv6 traffic on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 access-group Private6 in**

ipv6 access-policy *<ipv6 acp>*

Use the **ipv6 access-policy** command to assign a specified Internet Protocol version 6 (IPv6) access control policy (ACP) to an interface. IPv6 ACPs are applied to IPv6 traffic entering an interface. Use the **no** form of this command to remove an ACP association.

Syntax Description

<ipv6 acp>	Identifies the configured IPv6 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv6 ACPs associated with an interface.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example applies the IPv6 ACP **PRIVATEv6** to the interface:

Enable the AOS security features:
(config)**#ipv6 firewall**

Associate the ACP with the Frame Relay subinterface 1.16:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 access-policy PRIVATEv6**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 2826*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 2826*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the interface and enables IPv6 processing on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address *<ipv6 link-local address>* link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 link-local address>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the interface.

Default Values

By default, no IPv6 address is configured for the interface and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

A single link-local address can be manually configured on an interface. The lower 64 bits of the specified address become the Interface ID for the interface, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the interface and can be derived from the interface's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the interface.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example manually creates a link-local IPv6 address on the interface and enables IPv6 processing:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 address autoconfig

Use the **ipv6 address autoconfig** command to enable Internet Protocol version 6 (IPv6) processing on the interface, create a local-link IPv6 address for the interface, and allow the interface to automatically configure itself based on advertisements from other routers on the link. Use the **no** form of this command to remove all autoconfigured addresses, prefixes, and any resulting routes from the interface and also causes the interface to cease processing received router advertisements (RAs).Variations of this command include:

ipv6 address autoconfig
ipv6 address autoconfig default
ipv6 address autoconfig default metric <*value*>

Syntax Description

default	Optional. Specifies that the interface maintain a list of advertising routers that are willing to be IPv6 default routers.
metric <*value*>	Optional. Specifies the administrative distance for a default router maintained in the default router list. Range is **1** to **255**. Routes with lower administrative distance are favored.

Default Values

By default, no IPv6 addresses are configured for the interface and IPv6 processing is not enabled. When an IPv6 address is configured automatically, the administrative distance for default routers is **2** by default.

Command History

Release 18.1	Command was introduced.

Functional Notes

When autoconfiguration is enabled, the interface listens for RA messages that tell the interface how it should be configured. The interface then creates addresses for advertised 64-bit prefixes with the A flag in the IPv6 address set using stateless address autoconfiguration (SLAAC). The addresses use the EUI-64 interface ID in the lower 64 bits of the address. A route type of *Connected* is added to the route table if the L flag on the prefix advertisement (on-link flag) is also set.

Usage Examples

The following example enables IPv6 processing on the interface, creates a link-local IPv6 address for the interface, and allows the interface to automatically configure itself for IPv6:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 address autoconfig**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname <*partial fqdn*>
ipv6 address dhcp hostname fqdn <*fqdn*>
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 2821*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 address 2001:DB8:1::1/64**
(config-fr 1.16)**#ipv6 address dhcp fqdn client@company.com**

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*

Use the **ipv6 address named-prefix** command to create an Internet Protocol version 6 (IPv6) address for the interface using the values in a named prefix. Use the **no** form of this command to remove the address from the interface. Variations of this command include:

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*
ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>* **eui-64**

Syntax Description

<prefix name>	Specifies the named prefix to use to create the address.
<ipv6 address/prefix-length>	Specifies the address portion appended to the named prefix to create a 128-bit host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
eui-64	Optional. Indicates that the interface ID is to be placed in the lower 64 bits of the address.

Default Values

By default, no IPv6 addresses are specified on the interface.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example creates an IPv6 address on the interface using the named prefix **PREFIX1**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 address named-prefix PREFIX1 2001:1:0:/48**

ipv6 crypto map *<name>*

Use the **ipv6 crypto map** command to associate Internet Protocol version 6 (IPv6) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

Syntax Description

<name>	Specifies the IPv6 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Only one IPv6 crypto map can be specified per interface, and the crypto map is applied within the virtual routing and forwarding (VRF) instance to which the interface belongs. To apply the IPv6 crypto map, the interface must have IPv6 enabled. In addition, the interface must have an IPv6 address of appropriate scope to allow connectivity to peer's addresses as specified in the crypto map's entries.

Usage Examples

The following example applies all IPv6 crypto maps with the name **MyMap** to the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6**
(config-fr 1.16)**#ipv6 crypto map MyMap**

ipv6 dhcp client information refresh minimum <*seconds*>

Use the **ipv6 dhcp client information refresh minimum** command to specify the minimum value the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the interface accepts as its information refresh timer. Use the **no** version of this command to return to the default setting.

Syntax Description

<*seconds*>	Specifies the refresh timer in seconds. Valid range is **600** to **3600** seconds.

Default Values

By default, the DHCPv6 client refresh timer is set to **600** seconds.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example specifies the DHCPv6 client refresh timer for the interface is **800** seconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 dhcp client information refresh minimum 800**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 dhcp client pd PREFIX1**

ipv6 dhcp relay destination *<ipv6 address>*

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination *<ipv6 address>*
ipv6 dhcp relay destination *<ipv6 address>* *<interface>*
ipv6 dhcp relay destination *<ipv6 address>* **mef-ethernet** *<slot/port>*
ipv6 dhcp relay destination *<ipv6 address>* **system-control-evc**
ipv6 dhcp relay destination *<ipv6 address>* **system-management-evc**

Syntax Description

<ipv6 address>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** *<ipv6 address>* **?** to display a list of valid interfaces.
mef-ethernet *<slot/port>*	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC) is used when sending messages to the DHCPv6 server.
system-management-evc	Optional. Specifies the system management EVC is used when sending messages to the DHCPv6 server.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command *ipv6 on page 2821*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6**
(config-fr 1.16)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped mulitcast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the interface and specify that the interface is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the interface, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the interface. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this interface. All DHCPV^ requests received on this interface are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Enabling the interface as a DHCPv6 server using this command places the interface into DHCPv6 server mode. DHCPv6 modes (server or relay) are mutually exclusive at the interface. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the interface as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 address 2001:DB8:1::1/64**
(config-fr 1.16)**#ipv6 dhcp server POOL1**

ipv6 ffe

Use the **ipv6 ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 6 (IPv6) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 ffe
ipv6 ffe max-entries <*value*>

> NOTE *Issuing this command will cause all RapidRoute entries to be cleared from this IPv6 interface.*

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled on IPv6-enabled interfaces (using the command *ipv6 on page 2231*). The default number of **max-entries** is **4096**.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv6 interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#no ipv6 ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the interface in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the interface.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the interface in host mode:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 mode host unicast**

ipv6 mtu *<size>*

Use the **ipv6 mtu** command to specify the maximum transmission unit (MTU) for Internet Protocol version 6 (IPv6) packets on the interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Specifies the MTU value. Valid range is **1280** to **1500** bytes.

Default Values

By default, the MTU of the interface is set to **1280** bytes.

Command History

Release 18.1	Command was introduced.

Functional Notes

In IPv6, the minimum MTU is 1280 octets. Any link that has an MTU less than 1280 octets must use link fragmentation and reassembly that is transparent to IPv6 (for example, the Fragmentation Header). Sources in the IPv6 network are expected to perform path maximum transmission unit (PMTU) discovery to send packets larger than 1280 octets. PMTU works in the following manner: First, the sending node assumes the link MTU of the interface from which the traffic is being forwarded and then sends the IPv6 packet at the link MTU size. If a router on the path is unable to forward the packet, it sends an ICMP *Packet Too Big* message back to the sending node containing the link MTU of the link on which the packet forwarding failed. The sending node then rests the PMTU to the value of the MTU field in the Internet Control Message Protocol version 6 (ICMPv6) *Packet Too Big* message, and the packet is resent.

The MTU for IPv6 packets can be set on a per-interface basis. There are two methods for setting MTUs for interfaces if required: one for Layer 3 interfaces, and one for the underlying Layer 1 and Layer 2 interfaces. For all interface types, use the **ipv6 mtu** *<size>* command to specify the IPv6 MTU in bytes from the interface's configuration mode. The minimum MTU setting for IPv6 is **1280** bytes, and the maximum is **1500** bytes. The IPv6 MTU value is independent of the IPv4 MTU setting (set with the command *ip mtu <size> on page 2801*).

When the interface is forwarding the IPv6 packet as a router, if the packet size exceeds the IPv6 MTU of the egress interface, the packet is dropped and ICMPv6 *Packet Too Big* message is sent to the source. When originating an IPv6 packet from the local IPv6 stack, and the packet is larger than the IPv6 MTU of the egress interface, the packet is fragmented and sent.

Usage Examples

The following example specifies the IPv6 MTU value for the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 mtu 1350**

ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** command to specify that the Advertisement Interval Option is sent in Internet Protocol version 6 (IPv6) router advertisement (RA) messages from the router. This command is effectual only when the interface is in router mode. Use the **no** form of this command to return to the default interval.

Syntax Description

No subcommands.

Default Values

By default, Advertisement Interval Options are not sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

Sending the Advertisement Interval Option should be enabled when the router is functioning in a mobile IP environment to aid movement detection by mobile nodes. This option contains the current value of the maximum router advertisement interval configured using the command *ipv6 nd ra interval on page 2852*.

Usage Examples

The following example specifies that the interface include Advertisement Interval Options in RA messages sent from the router:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd advertisement-interval**

ipv6 nd cache max-incomplete <*number*>

Use the **ipv6 nd cache max-incomplete** command to specify the maximum number of incomplete entries the Neighbor Discovery (ND) cache retains. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of incomplete ND entries to retain in the cache. Valid range is **1** to **321**.

Default Values

By default, the incomplete ND entries can take at maximum one-third of the possible ND cache entries (varies by product).

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example specifies that the interface stores **150** incomplete entries in the ND cache:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd cache max-incomplete 150**

ipv6 nd dad attempts <*number*>

Use the **ipv6 nd dad attempts** command to specify the number of neighbor solicitation (NS) messages sent by the interface when performing Internet Protocol version 6 (IPv6) duplicate address detection (DAD). This command is effectual when the interface is in either host or router mode. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of NS messages that will be sent. Range is **0** to **10** messages. A value of **0** disables DAD on the interface.

Default Values

By default, the interface sends **1** NS message.

Command History

Release 18.1	Command was introduced.

Functional Notes

DAD is used by devices to determine if IPv6 addresses are unique before they are applied to interfaces. DAD is used in NS messages to detect duplicate unicast addresses. The Target Address fields in the NS messages are set to the IPv6 address for which duplication is being detected. Destination IPv6 addresses for DAD in NS messages are the solicited-node multicast version of the address being tested. Source IPv6 addresses for DAD are set to the IPv6 unspecified address (::). Once the IPv6 address is determined by DAD to be unique, it can be applied to the IPv6 interface on the node.

DAD in AOS is performed when an interface transitions state from DOWN to UP or when manually configuring an address. When performing DAD because of an interface transition, DAD will happen immediately after the interface transition and again 40 seconds later to cooperate with the port being connected to an Ethernet switch.

Usage Examples

The following example specifies that **3** NS messages are sent by the interface when performing DAD:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd dad attempts 3**

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command to specify the M flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. The M flag instructs hosts receiving the RA that they can use stateful Dynamic Host Configuration Protocol version 6 (DHCPv6) to configure addresses and nonaddress information. Use the **no** form of this command to disable the setting of the M flag.

Syntax Description

No subcommands.

Default Values

By default, the M flag is not set in RAs.

Command History

Release 18.1	Command was introduced.

Functional Notes

If you specify that the M flag is set in RA messages, you do not need to set the 0 flag (it becomes redundant).

Usage Examples

The following example sets the M flag for RA messages sent by the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd managed-config-flag**

ipv6 nd ns-interval *<value>*

Use the **ipv6 nd ns-interval** command to specify the interval between transmission of certain Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages and to control what ND value is advertised in router advertisement (RA) messages. This command is effectual whether the interface is in host or router mode. Use the **no** form of this command to return the interval to the default value.

Syntax Description

<value>	Specifies the time (in milliseconds) between neighbor message transmissions. Valid range is **1000** to **3600000** ms.

Default Values

By default, the interval is set to **1000** ms for internal use by the router and **0** (unspecified) is sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command controls the spacing of neighbor solicitation (NS) messages for functions such as address resolution, reachability detection, and duplicate address detection (DAD). For DAD it also serves as the amount of time after the last transmission before the detection phase of autoconfiguration terminates. In addition, the command controls the interval between unsolicited neighbor advertisement (NA) messages.

Usage Examples

The following example changes the interval between RA messages sent from the interface to **2000** ms:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd ns-interval 2000**

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command to specify the O flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. When the O flag is set, hosts receiving the RA messages are instructed that they may use stateless Dynamic Host Configuration Protocol version 6 (DHCPv6) to receive information that is not IPv6 addressing information, and to use some other method (whether through manual configuration, stateless address autoconfiguration (SLAAC), etc.) for addressing information. Use the **no** form of this command to disable the O flag setting.

Syntax Description

No subcommands.

Default Values

By default, the O flag is not set in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

If the M flag is set for RA messages, you do not need to set the O flag.

Usage Examples

The following example sets the O flag in RA messages from the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd other-config-flag**

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the interface. Use the **no** form of this command to remove the specified prefix configuration from the interface. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the interface is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the interface. Prefixes for IPv6 addresses configured on a router interface are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the interface.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ipv6 nd purge-timer <*value*>

Use the **ipv6 nd purge-timer** command to specify the maximum amount of time an unused Internet Protocol version 6 (IPv6) neighbor entry remains in the neighbor cache. This command applies to interfaces in either host or router mode. Use the **no** form of this command to return the purging interval to the default value.

Syntax Description

<*value*>	Specifies the neighbor cache entry storage time in minutes. Valid range is **10** to **1440** minutes.

Default Values

By default, idle (STALE) neighbor cache entries are cleared after **1440** minutes (24 hours).

Command History

Release 18.1	Command was introduced.

Functional Notes

This command applies to interfaces in either router or host mode. A neighbor entry is typically purged when neighbor unreachability detection (NUD) is invoked and the neighbor is determined to no longer be reachable. However, NUD is not performed on idle (STALE) neighbor entries, so this command provides a method for purging unused entries after a specified amount of time.

Usage Examples

The following example specifies that idle neighbor entries in the neighbor cache are removed after **800** minutes:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd purge-timer 800**

ipv6 nd ra interval

Use the **ipv6 nd ra interval** command to specify the interval between transmission of Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 nd ra interval *<max time>*
ipv6 nd ra interval *<max time> <min time>*
ipv6 nd ra interval msec *<max time>*
ipv6 nd ra interval msec *<max time> <min time>*

Syntax Description

<max time>	Specifies the maximum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **4** to **1800** seconds and **70** to **1800000** ms.
<min time>	Optional. Specifies the minimum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **3** seconds to 75 percent of the configured maximum time value in seconds, or **30** ms to 75 percent of the configured maximum time value in ms.
msec	Optional. Specifies that the time values are in milliseconds.

Default Values

By default, the interval is set in seconds and has a maximum interval time of **200** seconds and a minimum interval time of 75 percent of the maximum seconds value, but not less than **3** seconds.

Command History

Release 18.1	Command was introduced.

Functional Notes

If this router is used as a default router, the interval between RA messages should not be set to a larger value than the RA lifetime set by the command *ipv6 nd ra lifetime <value> on page 2853*, which has a default value of **1800** seconds.

Usage Examples

The following example specifies that the maximum interval in seconds between RA message transmissions is **300**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd ra interval 300**

ipv6 nd ra lifetime <*value*>

Use the **ipv6 nd ra lifetime** command to specify the router lifetime advertised in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is effectual when the interface is in router mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

ipv6 nd ra lifetime <*value*>
ipv6 nd ra lifetime default-route

Syntax Description

<*value*>	Specifies the router lifetime in seconds. Range is **0** to **9000** seconds. A value of **0** indicates this is not a default router. A value other than 0 indicates to other nodes that this router can be used as a default router.
default-route	Specifies the RA lifetime is **0** if no default route exists on any IPv6 interface.

Default Values

By default, the router lifetime is set to **1800** seconds.

Command History

Release 18.1	Command was introduced.
Release R11.5.0	Command was expanded to include the **default-route** parameter.

Functional Notes

A value other than **0** for a router lifetime should be larger than the router advertisement interval specified in the command *ipv6 nd ra interval on page 2852*.

Usage Examples

In the following example, the router lifetime advertised in RA messages is **3000** seconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd ra lifetime 3000**

ipv6 nd ra reachable-time <*value*>

Use the **ipv6 nd ra reachable-time** command to specify the value advertised for reachable time in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command also specifies the internal base reachable time used by the router. This command is effectual for interfaces in either host or router mode. Use the **no** form of this command to return the reachability value to the default setting.

Syntax Description

<*value*>	Specifies the reachability time in milliseconds. Range is **0** to **3600000** ms. A value of **0** indicates the reachable time is unspecified.

Default Values

By default, the router advertises a reachability time of **0** ms and uses an internal value of **30000** ms.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command is effectual for interfaces in either router or host mode. For hosts, this value sets the internal reachable time used by the host if no RAs are received specifying a different value. For routers, the value indicates the amount of time a device is considered reachable after having received a reachability confirmation in neighbor unreachabililty detection (NUD).

Usage Examples

The following example specifies that a reachability time of **50000** ms is advertised in RA messages:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd ra reachable-time 50000**

ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command to specify whether Internet Protocol version 6 (IPv6) router advertisement (RA) messages will be suppressed. This command only applies to interfaces in router mode. Use the **no** form of this command to begin sending RA messages.

Syntax Description

No subcommands.

Default Values

By default, RA messages are not suppressed. When IPv6 routing is not enabled on the router, or when implemented in a host-only mode, the default setting is to suppress advertisements on all interface types.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example suppresses RA messages on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd ra suppress**

ipv6 nd router-preference

Use the **ipv6 nd router-preference** command to specify the default router preference value set in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. Setting this preference helps the receivers of RA messages to determine the preference of one router over another as a default router in environments with multiple routers. Use the **no** form of this command to return the preference to the default setting. Variations of this command include:

ipv6 nd router-preference high
ipv6 nd router-preference low
ipv6 nd router-preference medium

Syntax Description

high	Specifies the preference value is high.
low	Specifies the preference value is low.
medium	Specifies the preference value is medium.

Default Values

By default, the router preference is set to medium.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that the advertised default router preference is high:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 nd router-preference high**

ipv6 route-cache

Use the **ipv6 route-cache** command to enable Internet Protocol version 6 (IPv6) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 18.2	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Fast switching allows an IPv6 interface to provide optimum performance when processing IPv6 traffic.

Usage Examples

The following example enables IPv6 fast switching on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ipv6 route-cache**

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the Frame Relay subinterface to receive LLDP packets:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to disable this feature. Variations of this command include:

lldp send
lldp send management-address
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

By default, all interfaces are configured to transmit and receive LLDP packets of all types.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the Frame Relay subinterface to transmit LLDP packets containing all enabled information types:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#lldp send**

The following example configures the Frame Relay subinterface to transmit and receive LLDP packets containing all information types:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#lldp send-and-receive**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip primary vrrp <*number*>
media-gateway ip primary vrrpv3 <*number*>
media-gateway ip secondary <*ipv4 address*>
media-gateway ip secondary vrrp <*number*>
media-gateway ip secondary vrrp <*number*> <*ipv4 address*>
media-gateway ip secondary vrrpv3 <*number*>
media-gateway ip secondary vrrpv3 <*number*> <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrrp <*number*>	Specifies that the IPv4 address of the Virtual Router Redundancy Protocol version 2 (VRRP) router group's virtual router ID (VRID) is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
vrrpv3 <*number*>	Specifies that the IPv4 address of the VRRP version 3 (VRRPv3) VRID is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
<*ipv4 address*>	Optional. Specifies a secondary IPv4 address of the VRRP or VRRPv3 VRID is used as the media gateway address on the interface. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A4.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.
Release R12.2.0	Command was expanded to include the **vrrp** and **vrrpv3** parameters.

Functional Notes

To use VRRP or VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRP or VRRPv3.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#media-gateway ip primary**

media-gateway ipv6

Use the **media-gateway ipv6** command to associate an Internet Protocol version 6 (IPv6) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv6 address associated with it. However, some interfaces allow dynamic configuration of IPv6 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ipv6
media-gateway ipv6 <*ipv6 address*>
media-gateway ipv6 loopback <*interface id*>
media-gateway ipv6 vrrpv3 <*number*>
media-gateway ipv6 vrrpv3 <*number*> <*ipv6 address*>

Syntax Description

<*ipv6 address*>	Specifies an IPv6 address to use for the media gateway. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
loopback <*interface id*>	Specifies an IPv6 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv6 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
vrrpv3 <*number*>	Specifies that all the secondary IPv6 addresses of the Virtual Routing Redundancy Protocol version 3 (VRRPv3) virtual router ID (VRID) are used as media gateway addresses on the interface. Valid VRID range is **1** to **255**.
<*ipv6 address*>	Optional. Specifies a single IPv6 address of the VRRPv3 VRID is used as the media gateway address on the interface. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

Default Values

By default, **media-gateway ipv6** is disabled.

Command History

Release R10.8.0	Command was introduced.
Release R12.2.0	Command was expanded to include the **vrrpv3** parameters.

Functional Notes

To use VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRPv3.

Usage Examples

The following example configures the unit to use the IPv6 address for RTP traffic:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#media-gateway ipv6**

ospfv3 <*process id*> **area** <*area id*>

Use the **ospfv3 area** command to add an interface to an Open Shortest Path First version 3 (OSPFv3) process, and to configure the OSPFv3 process on the interface. This command places the interface in the specified area for the specified Internet Protocol version 6 (IPv6) OSPFv3 address family, and optionally defines the instance ID that is used to represent this OSPFv3 process in messages on the interface's link. Use the **no** form of this command to remove the OSPFv3 process from the interface. Variations of this command include:

ospfv3 <*process id*> **area** <*area id*> **ipv6**
ospfv3 <*process id*> **area** <*area id*> **ipv6 instance** <*instance id*>

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join, for the specified address family. The process ID is locally significant to the device, and must be unique among all OSPFv3 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the given OSPFv3 process. Valid range is **0** to **4294967295**.
ipv6	Identifies the OSPFv3 address family as IPv6.
instance <*instance id*>	Optional. Specifies the value to use in the instance ID field of messages sent or received by this OSPFv3 process on the interface's link. Valid range is **0** to **31**.

Default Values

By default, an OSPFv3 process is not configured on an interface. By default, process IDs, area IDs, and instance IDs are not defined.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

When using this command to enable an OSPFv3 process on an interface, keep the following rules in mind:

- The interface must have the address family enabled on the interface. If the address family is not enabled on the interface, the command is rejected and an error is displayed.
- Only interfaces on the default virtual routing and forwarding (VRF) instance support this command. Interfaces on a nondefault VRF will display an error when you attempt to configure OSPFv3 settings.
- The interface and the specified OSPFv3 process (if defined in the global configuration) must be in the same VRF or the command will fail.
- The address family must match that specified for the OSPFv3 process if the process has been defined in the global configuration or the command will fail.
- If the OSPFv3 process identified by the process ID does not exist in the global configuration, it is automatically created, along with the specified address family, and it is assigned to the VRF of which the interface is a member.

- If the specified OSPFv3 process is already at its maximum limit of processes or address families, the command fails.
- If the specified OSPFv3 process already exists in the global configuration, but its configuration does not include an address family, the specified address family is added to the OSPFv3 router configuration.
- A given OSPFv3 process can only have one address family.
- Multiple OSPFv3 instances per address family, per VRF, can be created and can be assigned to a given interface.
- If the interface's VRF changes, all OSPFv3 assignments are removed.
- To change an OSPFv3 process's VRF, the process must first be removed and then recreated. Removing the process removes all OSPFv3 assignments for that process form all interfaces.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To add an interface to the OSPFv3 process **5**, in area **10**, with an instance ID of **10**, enter the command as follows:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 area 10 ipv6 instance 10**

ospfv3 authentication

Use the **ospfv3 authentication** command to authenticate an interface that is performing Internet Protocol version 6 (IPv6) Open Shortest Path First version 3 (OSPFv3) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ospfv3 authentication ipsec spi <*spi*> **md5** <*key*>
ospfv3 authentication ipsec spi <*spi*> **sha1** <*key*>
ospfv3 authentication null

Syntax Description

ipsec	Specifies that IP security (IPsec) authentication is used.
spi <*spi*>	Specifies the security parameter index (SPI). Valid range is **256** to **4294967295**.
md5 <*key*>	Specifies that MD5 authentication is used. Keys are specified in 32 hexadecimal characters.
sha1 <*key*>	Specifies that SHA-1 authentication is used. Keys are specified in 40 hexadecimal characters.
null	Specifies that no OSPFv3 authentication is used.

Default Values

By default, this is set to **null** (meaning no authentication is used).

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example specifies that no OSPFv3 authentication will be used on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 authentication null**

ospfv3 <*process id*> cost <*cost*>

Use the **ospfv3 cost** command to specify a value that represents the cost of sending an Open Shortest Path First version 3 (OSPFv3) packet over the interface. Use the **no** form of this command to return the cost to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
cost <*cost*>	Specifies the OSPFv3 cost of the interface. This value overrides any automatically computed cost value (default value). Valid range is **1** to **65535**.

Default Values

By default, the OSPFv3 cost of the interface is automatically computed. The automatic cost computation is the reference bandwidth divided by the interface bandwidth. The reference bandwidth is set by the command *auto-cost reference-bandwidth <value> on page 4150*, and defaults to **100** Mbps.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the OSPFv3 cost of the interface as **10**:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ospfv3 5 cost 10
```

ospfv3 <*process id*> dead-interval <*value*>

Use the **ospfv3 dead-interval** command to specify the maximum interval allowed between Open Shortest Path First version 3 (OSPFv3) Hello packets on the interface. If the maximum interval is exceeded, neighboring devices will assume that the device is down. This value must be the same across all interfaces on a link. Use the **no** form of this command to return the dead interval to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
dead-interval <*value*>	Specifies the maximum number of seconds allowed between OSPFv3 Hello packets. It is recommended that this value be **4** times the Hello packet interval (set with the command *ospfv3 <process id> hello-interval <value> on page 2872*). Valid range is **1** to **65535** seconds.

Default Values

By default, the maximum interval allowed between OSPFv3 Hello packets is set to **40** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To specify the dead interval between OSPFv3 Hello packets on the interface, enter the command as follows:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 dead-interval 100**

ospfv3 encryption

Use the **ospfv3 encryption** command to specify a symmetrical, bidirectional Open Shortest Path First version 3 (OSPFv3) security association (SA) that uses encapsulating security payload (ESP) for encryption and authentication of all OSPFv3 messages that are sent or received on the interface. This command allows you to specify OSPFv3 security at the interface level. Use the **no** form of this command to remove IP security (IPsec) protection of OSPFv3 messages on the interface. Variations of this command include:

ospfv3 encryption ipsec spi <*spi*> **esp** <*encryption type*> <*encryption key*> <*authentication type*> <*authentication key*>
ospfv3 encryption ipsec spi <*spi*> **esp null** <*authentication type*> <*authentication key*>
ospfv3 encryption null

Syntax Description

ipsec	Specifies that IPsec encryption is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by any other IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
esp	Specifies that ESP is used.
null	Specifies that OSPFv3 messages on this interface are not encrypted when used in the **ospfv3 encryption null** format (even when encryption is specified by the OSPFv3 area configuration). When used in the **ospfv3 encryption ipsec spi** <*spi*> **esp null** format, **null** indicates that messages on the interface will not be encrypted, but will be authenticated.
<*encryption type*>	Specifies the type of algorithm used to encrypt OSPFv3 messages. Valid values for encryption are: **3des** uses triple data encryption standard (DES). **aes-cbc** uses advanced encryption standard (AES) with cipher block chaining (CBC). Select from **aes-cbc 128**, **aes-cbc 192**, or **aes-cbc 256**. **des** uses DES.
<*encryption key*>	Specifies the hexadecimal encryption key. The size of the encryption key is determined by the respective encryption algorithm, as follows: **3des** uses a **48** character key size. **aes-cbc 128** uses a **32** character key size. **aes-cbc 192** uses a **48** character key size. **aes-cbc 256** uses a **64** character key size. **des** uses a **16** character key size.
<*authentication type*>	Specifies the algorithm used for authenticating OSPFv3 messages. Valid authentication methods are Message-Digest 5 (**md5**) and Secure-Hash 1 (**sha1**) algorithms.

<authentication key> Specifies the hexadecimal authentication key. The size of the authentication key is determined by the respective authentication algorithm, as follows:

md5 uses a **32** character key size.

sha1 uses a **40** character key size.

Default Values

By default, there is no security for OSPFv3 messages on an interface.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

This commands specifies OSPFv3 security at the interface level. Protection specified with this command overrides any area-level OSPFv3 protection that might apply to the interface.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages with an SPI of **120**, no encryption, and **md5** as the authentication method:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ospfv3 encryption ipsec spi 120 esp null md5
    NeWtStpsswdLoonGpsswDhtThmnWoKEY
```

ospfv3 <*process id*> hello-interval <*value*>

Use the **ospfv3 hello-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) Hello packets sent on the interface. This value must be the same across all interfaces on the link. Use the **no** form of this command to return the Hello packet interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
hello-interval <*value*>	Specifies the number of seconds allowed between OSPFv3 Hello packets. Valid range is **1** to **65535** seconds.

Default Values

By default, the Hello packet interval for OSPFv3 is **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the interval between OSPFv3 Hello packets on the interface is **20** seconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 hello-interval 20**

ospfv3 <*process id*> network

Use the **ospfv3 network** command to specify the network type for Open Shortest Path First version 3 (OSPFv3) enabled interfaces. Use the **no** form of this command to return the interface's network type to the default value. Variations of this command include:

ospfv3 <*process id*> **network broadcast**
ospfv3 <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
broadcast	Specifies that the OSPFv3 network type for the interface is set to broadcast.
point-to-point	Specifies that the OSPFv3 network type for the interface is set to point-to-point.

Default Values

By default, Ethernet interfaces are set to network type broadcast, and point-to-point (PPP), Frame Relay, and loopback interfaces are set to network type point-to-point.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the network interface as point-to-point:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 network point-to-point**

ospfv3 <*process id*> priority <*value*>

Use the **ospfv3 priority** command to specify the Open Shortest Path First version 3 (OSPFv3) priority for the interface. Use the **no** form of this command to return the interface's priority to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
priority <*value*>	Specifies the OSPFv3 priority for the interface. Valid range is **0** to **255**.

Default Values

By default, the OSPFv3 priority of an interface is set to **1**.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

Priority is used in the election of the designated router and backup designated router on multi-access networks. Interfaces connected to multi-access networks (such as Ethernet interfaces) perform an election for a designated and backup designated router. The router interface with the highest OSPFv3 priority on the link becomes the designated router for that link. The interface with the next highest priority becomes the designated backup router. In the event there is a tie, the router interface with the highest router ID takes precedence. A priority value of **0** indicates the router is ineligible to become either the designated or backup designated router.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's OSPFv3 priority value to **6**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 priority 6**

ospfv3 <*process id*> retransmit-interval <*value*>

Use the **ospfv3 retransmit-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) sent on the interface. Use the **no** form of this command to return the OSPFv3 LSA interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
retransmit-interval <*value*>	Specifies the number of seconds between OSPFv3 LSAs sent on the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA retransmit interval is set to **5** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the LSA retransmit interval is **10** seconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 retransmit-interval 10**

ospfv3 <*process id*> shutdown

Use the **ospfv3 shutdown** command to disable an Open Shortest Path First version 3 (OSPFv3) process on the interface. When this command is used, the OSPFv3 commands remain in place, but logically it appears to the interface as though the OSPFv3 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv3 process.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables OSPFv3 process **5** on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 shutdown**

ospfv3 <*process id*> transmit-delay <*value*>

Use the **ospfv3 transmit-delay** command to specify the estimated time that is required to propagate an Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) on the interface. Use the **no** form of this command to return the transmit delay to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 2865*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
transmit-delay <*value*>	Specifies the number of seconds required to send LSAs from the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA transmit delay is set to **1** second.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's LSA transmit delay to **2** seconds:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#ospfv3 5 transmit-delay 2**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the Frame Relay interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#rtp quality-monitoring**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.9	Command was expanded to the Frame Relay and the ATM subinterfaces.

Usage Examples

The following example enables SNMP on the virtual Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.9	Command was explanded to the Frame Relay and the ATM subinterfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#no snmp trap link-status**

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** command to block bridge protocol data units (BPDUs) from being transmitted and received on this interface. To return to the default value, use the **no** form of this command. Variations of this command include:

spanning-tree bpdufilter disable
spanning-tree bpdufilter enable

Syntax Description

disable	Disables the BPDU filter.
enable	Enables the BPDU filter.

Default Values

By default, this command is set to disable.

Command History

Release 5.1	Command was introduced.

Functional Notes

The purpose of this command is to remove a port from participation in the spanning tree. This might be beneficial while debugging a network setup. It normally should not be used in a live network.

Usage Examples

The following example enables the BPDU filter on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#spanning-tree bpdufilter enable**

spanning-tree bpduguard

Use the **spanning-tree bpduguard** command to block bridge protocol data units (BPDUs) from being received on this interface. To return to the default value, use the **no** form of this command. Variations of this command include:

spanning-tree bpduguard disable
spanning-tree bpduguard enable

Syntax Description

disable	Disables the BPDU block.
enable	Enables the BPDU block.

Default Values

By default, this command is set to disable.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables the BPDU guard on the interface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#spanning-tree bpduguard enable**

spanning-tree edgeport

Use the **spanning-tree edgeport** command to set this interface to be an edgeport. This command overrides the global setting (refer to *spanning-tree edgeport default on page 1837*). Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, this command is set to disable.

Command History

Release 5.1	Command was introduced.
Release 8.1	Command was added to the ATM Subinterface command set.

Functional Notes

When an interface is designated as an edgeport, the interface will immediately go to a forwarding state when the link becomes active. When an interface is not designated as an edgeport, the interface must go through the listening and learning states before going to the forwarding state.

Usage Examples

The following example configures the interface to be an edgeport:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#spanning-tree edgeport**

An individual interface can be configured to not be considered an edgeport. For example:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#spanning-tree edgeport disable**

or

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#no spanning-tree edgeport**

spanning-tree link-type

Use the **spanning-tree link-type** command to configure the spanning-tree protocol link type for an interface. To return to the default value, use the **no** form of this command. Variations of this command include:

spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared

Syntax Description

auto	Determines link type by the port's duplex settings.
point-to-point	Manually sets link type to point-to-point regardless of duplex settings.
shared	Manually sets link type to shared regardless of duplex settings.

Default Values

By default, a port is set to auto.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command overrides the default link-type setting determined by the duplex of the individual port. By default, a port configured for half-duplex is set to **shared** link type, and a port configured for full-duplex is set to **point-to-point** link type. Setting the link type manually overrides the default and forces the port to use the specified link type. Using the **link-type auto** command, restores the convention of determining link type based on duplex settings.

Usage Examples

The following example forces the link type to point-to-point, even if the port is configured to be half-duplex:

(config)**#bridge 1 protocol ieee**
(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#spanning-tree link-type point-to-point**

Technology Review

Rapid transitions are possible in Rapid Spanning Tree Protocol (RSTP) by taking advantage of point-to-point links (a port is connected to exactly one other bridge) and edge-port connections (a port is not connected to any additional bridges). Setting the link type to **auto** allows the spanning tree to automatically configure the link type based on the duplex of the link. Setting the link type to **point-to-point** allows a half-duplex link to act as if it were a point-to-point link.

spanning-tree path-cost *<value>*

Use the **spanning-tree path-cost** command to assign a cost to a bridge group that is used when computing the spanning-tree root path. To return to the default path-cost value, use the **no** form of this command.

Syntax Description

<value>	Assigns a number to the bridge interface to be used as the path cost in spanning calculations. Valid range is **0** to **65535**.

Default Values

By default, the path-cost value is set to **19**.

Command History

Release 1.1	Command was introduced.
Release 8.1	Command was added to the ATM subinterface command set.
Release R10.1.0	Command was added to the Ethernet interface command set.

Functional Notes

The specified value is inversely proportional to the likelihood the bridge interface will be chosen as the root path. Set the path-cost value lower to increase the chance the interface will be the root. To obtain the most accurate spanning-tree calculations, develop a system for determining path costs for links and apply it to all bridged interfaces.

Usage Examples

The following example assigns a path cost of 100 on a Frame Relay subinterface:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#spanning-tree path-cost 100**

Technology Review

Spanning-tree protocol provides a way to prevent loopback or parallel paths in bridged networks. Using the priority values and path costs assigned to each bridging interface, the spanning-tree protocol determines the root path and identifies whether to block or allow other paths.

spanning-tree port-priority <*value*>

Use the **spanning-tree port-priority** command to select the priority level of a port associated with a bridge. To return to the default bridge-group priority value, use the **no** form of this command.

Syntax Description

<*value*>	Priority value for the bridge group; the lower the value, the higher the priority. Valid range is **0** to **255**.

Default Values

By default, the bridge-group priority value is set at **28**.

Command History

Release 1.1	Command was introduced.

Functional Notes

The only time that this priority level is used is when two interfaces with a path to the root have equal cost. At that point, the level set in this command will determine which port the bridge will use. Set the priority value lower to increase the chance the interface will be used.

Usage Examples

The following example sets the maximum priority on the Frame Relay subinterface labeled 1.16:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#spanning-tree port-priority 0**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<*name*>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the **frame-relay 1.16** interface to the VRF instance named **RED**:

(config)**#interface frame-relay 1.16**
(config-fr 1.16)**#vrf forwarding RED**

HDLC INTERFACE COMMAND SET

To create a virtual high level data link control (HDLC) interface and/or activate the HDLC Interface Configuration mode, enter the **interface hdlc** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface hdlc 1
(config-hdlc 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

alias link "<text>" on page 2890
bandwidth <value> on page 2891
bridge-group <value> on page 2892
bridge-group <number> vlan-transparent on page 2893
dial-backup commands begin on page 2894
dynamic-dns on page 2911
fair-queue on page 2913
hold-queue <value> out on page 2914
ip commands begin on page 2915
ipv6 dhcp relay destination <ipv6 address> on page 2955
keepalive <value> on page 2956
lldp receive on page 2957
lldp send on page 2958
max-reserved-bandwidth <value> on page 2960
media-gateway ip on page 2961
packet-capture <name> on page 2962
qos-policy on page 2963
rtp quality-monitoring on page 2965

snmp trap link-status on page 2966
vrf forwarding <name> on page 2967

alias link "*<text>*"

Each configured high level data link control (HDLC) interface (when referenced using Signaling Network Management Protocol (SNMP)) contains a link (physical port) and a bundle (group of links). RFC 1471 (for Link Connection Protocol) provides an interface table to manage lists of bundles and associated links. The **alias link** command provides the management station an identifying description for each link (HDLC physical).

Syntax Description

"*<text>***"**	Describes the interface (for SNMP) using an alphanumeric character string enclosed in quotation marks.

Default Values

By default, the HDLC identification string appears as empty quotation marks (" ").

Command History

Release 10.1	Command was introduced.

Functional Notes

The **alias link** string should be used to uniquely identify an HDLC link. Enter a string that clearly identifies the link.

Usage Examples

The following example defines a unique character string for the virtual HDLC interface (1):

(config)**#interface hdlc 1**
(config-hdlc 1)**#alias link "HDLC_link_1"**

Technology Review

Please refer to RFC 1990 for a more detailed discussion on HDLC links and bundles.

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies the bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view the default values, use the command *show interfaces on page 673*.

Command History

Release 9.1	Command was introduced.

Functional Notes

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 2960*) to adjust the bandwidth appropriately for QoS configurations.

Usage Examples

The following example sets bandwidth of the high level data link control (HDLC) interface to 10 Mbps:

(config)**#interface hdlc 1**
(config-hdlc 1)**#bandwidth 10000**

bridge-group *<value>*

Use the **bridge-group** command to assign an interface to the specified bridge group. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<value>	Specifies the bridge group (by number) to which to assign this interface. Range is **1** to **255**.

Default Values

By default, there are no configured bridge groups.

Command History

Release 9.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (Ethernet to T1 bridge, Ethernet to Frame Relay subinterface, etc.).

Usage Examples

The following example assigns the high level data link control (HDLC) interface labeled 1 to bridge group 1:

(config)**#interface hdlc 1**
(config-hdlc 1)**#bridge-group 1**

bridge-group <*number*> vlan-transparent

Use the **bridge-group vlan-transparent** command to prevent an interface from removing the virtual local area network (VLAN) tag. Use the **no** form of this command to allow the interface to remove the VLAN tag from the packet.

*The **bridge-group vlan-transparent** command is not a global command. The command must be applied on all interfaces of the bridge group.*

Syntax Description

<number>	Specifies the bridge group number. Valid range is **1** to **255**.

Default Values

By default, VLAN tags are removed from the data.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the high level data link control (HDLC) interface and Frame Relay subinterface.

Usage Examples

The following example removes the VLAN tags from the packets on the HDLC 1 interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#bridge-group 1 vlan-transparent**

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the interface to automatically attempt a dial backup upon failure. Use the **no** form of this command to disable this feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2897*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial backup upon a failure.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example enables automatic dial backup on the endpoint:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup auto-backup**

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2897*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to automatically restore the primary connection when the failure condition clears:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup auto-restore**

dial-backup backup-delay *<value>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 2897*.

Syntax Description

<value>	Specifies the delay period (in seconds) a failure must be active before AOS will enter backup operation on the interface. Range is **10** to **86400** seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **60** seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup backup-delay 60**

dial-backup call-mode

Use the **dial-backup call-mode** command to specify whether the configured backup interface answers or originates (or a combination of both) backup calls. Use the **no** form of this command to return to the default value. Variations of this command include:

dial-backup call-mode answer
dial-backup call-mode answer-always
dial-backup call-mode originate
dial-backup call-mode originate-answer
dial-backup call-mode originate-answer-always

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer**.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Functional Notes

The majority of the configuration for AOS dial-backup implementation is configured via the dial-backup PPP interface configuration commands. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname “Remote3200”
enable password adtran
!
interface eth 0/1
  ip address 192.168.1.254 255.255.255.0
  no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
```



```
  coding b8zs
  framing esf
  clock source line
  tdm-group 1 timeslots 1-24
  no shutdown
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.16 point-to-point
  frame-relay interface-dlci 16
  ip address 10.1.1.2 255.255.255.252
  dial-backup call-mode originate
  dial-backup number 5551111 analog ppp1
  dial-backup number 5552222 analog ppp1
no shutdown
!
interface ppp 1
  ip address  172.22.56.1  255.255.255.252
  ppp authentication chap
 username remoterouter password remotepass
 ppp chap hostname localrouter
  ppp chap password adtran
  no shutdown
!
ip route 192.168.2.0 255.255.255.0 172.22.56.2 255.255.255.252
!
line telnet 0 4
  password password
```

Sample configuration for central router (dialing in)

```
hostname “Central3200”
enable password adtran
!
interface eth 0/1
  ip address  192.168.100.254  255.255.255.0
  no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
  coding b8zs
  framing esf
  clock source line
```



```
  tdm-group 1 timeslots 1-24
  no shutdown
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.100 point-to-point
  frame-relay interface-dlci 100
  ip address 10.1.1.1 255.255.255.252
  dial-backup call-mode answer
  dial-backup number 555-8888 analog ppp 1
!
interface ppp 1
  ip address  172.22.56.2 255.255.255.252
  ppp authentication chap
 username localrouter password adtran
 ppp chap hostname remoterouter
 ppp chap password remotepass
  no shutdown
!
ip route 192.168.1.0 255.255.255.0 172.22.56.1 255.255.255.252

line telnet 0 4
  password password
```

Usage Examples

The following example configures AOS to generate backup calls for this endpoint using an analog modem interface (to phone number 555 1111), but never answer calls and specifies **ppp 1** as the backup interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#dial-backup call-mode originate
(config-hdlc 1)#dial-backup number 555 1111 analog ppp 1
```

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial backup, where in the configuration AOS accesses specific routing information, etc.):

Dialing Out

1. AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the dial-backup number command (refer to *dial-backup number <number> on page 2904*).
3. When placing the call, AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, AOS places a call to the second number (if a second number is configured). The second number to be dialed references a separate PPP interface.

Dialing In

1. AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from caller ID, the call is terminated.

dial-backup connect-timeout <*value*>

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*.

Syntax Description

<*value*>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call. Valid range is **10** to **300** seconds.

Default Values

By default, the **dial-backup connect-timeout** period is set to **60** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **120** seconds before retrying a failed dial-backup call:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup connect-timeout 120**

dial-backup force

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*. Variations of this command include:

dial-backup force backup
dial-backup force primary

Syntax Description

backup	Forces backup regardless of primary link state.
primary	Forces primary link regardless of its state.

Default Values

By default, this feature is disabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to force this interface into dial backup:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup force backup**

dial-backup maximum-retry <*value*>

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*.

Syntax Description

<*value*>	Selects the number of call retry attempts that will be made after a link failure. Valid range is **0** to **15** attempts. Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to **0** attempts.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to retry a dial-backup call four times before considering backup operation not available:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup maximum-retry 4**

dial-backup number <*number*>

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. Use the **no** form of this command to remove a configured dial-backup number. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*. Variations of this command include:

dial-backup number <*number*> **analog ppp** <*interface*>
dial-backup number <*number*> **digital-56k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>
dial-backup number <*number*> **digital-64k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>

Syntax Description

<*number*>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates the number connects to an analog modem.
digital-56k	Indicates the number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates the number belongs to a digital 64 kbps per DS0 connection.
<*isdn min chan*>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
<*isdn max chan*>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
ppp <*interface*>	Specifies the Point-to-Point Protocol (PPP) interface to use as the backup for this interface (for example, **ppp 1**).

Default Values

By default, there are no configured dial-backup numbers.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.
Release 17.2	Command was expanded to include the cellular connections.
Release 17.3	Cellular connections were removed from this command.

Usage Examples

The following example configures AOS to dial **704-555-1212** (digital 64 kbps connection) to initiate dial-backup operation for this endpoint using the configured **ppp 1** backup interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup number 7045551212 digital-64k 1 1 ppp 1**

dial-backup priority <*value*>

Use the **dial-backup priority** command to select the backup priority for this interface. This allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*.

Syntax Description

<*value*>	Sets the relative priority of this link. Valid range is **0** to **100**. A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to **50**.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example assigns the highest priority to this endpoint:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup priority 100**

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*.

Syntax Description

No subcommands.

Default Values

By default, AOS does not randomize the dial-backup call timers.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to randomize the dial-backup timers associated with this endpoint:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup randomize-timers**

dial-backup redial-delay <*value*>

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*.

Syntax Description

<*value*>	Specifies the delay in seconds between attempting to redial a failed backup attempt. Range is **10** to **3600** seconds.

Default Values

By default, **dial-backup redial-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures a redial delay of **25** seconds on this endpoint:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup redial-delay 25**

dial-backup restore-delay *<value>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is bouncing in and out of alarm. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*.

Syntax Description

<value>	Specifies the number of seconds AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range is **10** to **86400** seconds.

Default Values

By default, **dial-backup restore-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **30** seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup restore-delay 30**

dial-backup schedule

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial backup (as specified). For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*. Variations of this command include:

dial-backup schedule day <*name*>
dial-backup schedule enable-time <*value*>
dial-backup schedule disable-time <*value*>

Syntax Description

day <*name*>	Sets the days to allow backup. Valid range is Monday through Sunday.
enable-time <*value*>	Sets the time of day to enable backup. Time is entered in a 24-hour format (00:00).
disable-time <*value*>	Sets the time of day to disable backup. Time is entered in a 24-hour format (00:00).

Default Values

By default, dial backup is enabled for all days and times if the **dial-backup auto-backup** command has been issued and the dial-backup schedule has not been entered.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example enables dial backup Monday through Friday 8:00 a.m. to 7:00 p.m.:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup schedule enable-time 08:00**
(config-hdlc 1)**#dial-backup schedule disable-time 19:00**
(config-hdlc 1)**#no dial-backup schedule day Saturday**
(config-hdlc 1)**#no dial-backup schedule day Sunday**

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 2897*.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are disabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example deactivates the configured dial-backup interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dial-backup shutdown**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#dynamic-dns dyndns-custom host user pass**

fair-queue

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable first in, first out (FIFO) queueing for an interface. Variations of this command include:

fair-queue
fair-queue <*value*>

WFQ must be enabled on an interface to use priority queuing. By default, WFQ is enabled for all interfaces with maximum bandwidth speeds equivalent to T1/E1 and below.

Syntax Description

<*value*>	Optional. Value that specifies the maximum number of packets that can be present in each conversation subqueue. Packets received for a conversation after this limit is reached are discarded. Range is **16** to **512** packets.

Default Values

By default, fair queue is enabled with a threshold of **64** packets.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example enables WFQ on the interface with a threshold set at 100 packets:

(config)**#interface hdlc 1**
(config-hdlc 1)**#fair-queue 100**

hold-queue <*value*> out

Use the **hold-queue out** command to change the overall size of an interface's wide area network (WAN) output queue. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	The total number of packets the output queue can contain before packets are dropped. Range is **16** to **1000** packets.

Default Values

The default queue size for weighted fair queuing (WFQ) is 400. The default queue size for Point-to-Point Protocol (PPP) first in, first out (FIFO) and Frame Relay round-robin is 200.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example sets the overall output queue size to **700**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#hold-queue 700 out**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to create an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Assigned IPv4 ACL name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 9.1	Command was introduced.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the unit to only allow Telnet traffic (as defined in the user-configured **TelnetOnly** IP ACL) into the high level data link control (HDLC) interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#int hdlc 1**
(config-hdlc 1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

*Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the HDLC interface 1:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip access-policy PRIVATE**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address *<ipv4 address> <subnet mask>*
ip address *<ipv4 address> <subnet mask>* **secondary**

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 9.1	Command was introduced

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 /30**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip address 192.22.72.101 255.255.255.252 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

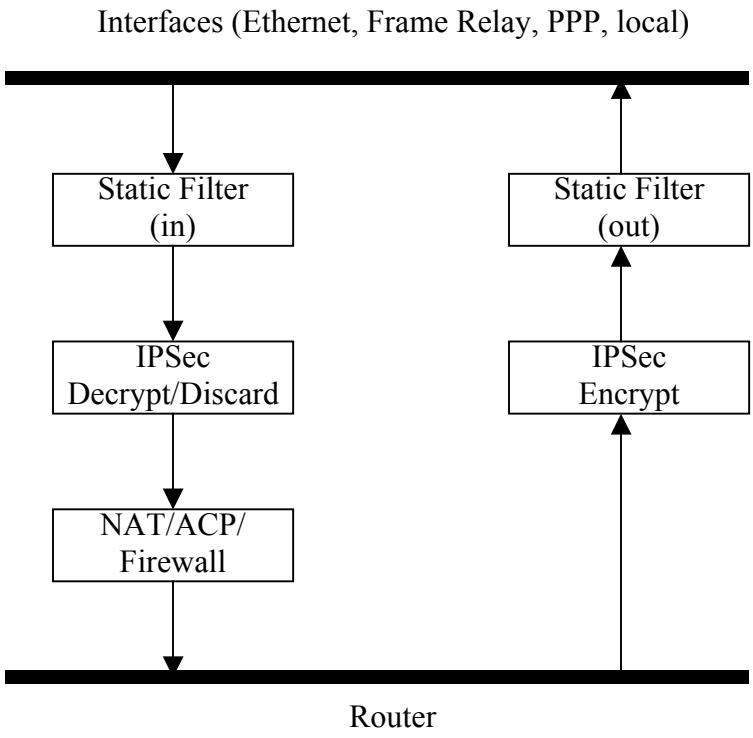
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#hdlc 1**
(config-hdlc 1)**#ip crypto map MyMap**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **hdlc 1**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute Engine on this interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries on this interface to be cleared.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **8192**.

Default Values

By default, the RapidRoute Engine is disabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the tunnel and high level data link control (HDLC) interface.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example enables RapidRoute and sets the maximum number of entries in the flow table to **50**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip ffe max-entries 50**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on an high level data link control (**HDLC)** interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper-address** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 9.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (**255.255.255.255**) or a subnet broadcast (for example, **192.33.4.251** for the **192.33.4.248 /30** subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface hdlc 1**
(config-hdlc 1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 9.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 2934* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the high level data link control (HDLC) interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip mcast-stub downstream
```


ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*address*> command (refer to *ip igmp on page 2929*) to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release 10.1	Command was expanded to include high level data link control (HDLC) interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 2931*, and *ip mcast-stub upstream on page 2934* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 9.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 2931* for more information.

Usage Examples

The following example enables multicast forwarding on the high level data link control (HDLC) interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip mcast-stub upstream
```


ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 9.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 9.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the high level data link control (HDLC) interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 9.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip ospf 1 network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the high level data link control (HDLC) 1 interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the high level data link control (HDLC) 1 interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip pim-sparse dr-priority 5**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the high level data link control (HDLC) 1 interface every **3600** seconds:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to **300** seconds:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the expected propagation delay to **300** milliseconds on the high level data link control (HDLC) 1 interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the high level data link control (HDLC) 1 interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 9.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the high level data link control (HDLC) interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the version command).

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the high level data link control (HDLC) interface to accept only RIP version 2 packets:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP **version 1** (the default value for the **version** command).

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the high level data link control (HDLC) interface to transmit only RIP version 2 packets:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast caching is enabled on all interfaces.

Command History

Release 9.1	Command was introduced.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the high level data link control (HDLC) interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 9.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Frame Relay Subinterface Configuration mode configures the Frame Relay subinterface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the high level data link control (HDLC) interface to use the IP address assigned to the Ethernet interface 0/1:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip unnumbered eth 0/1**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the high level data link control (HDLC) interface and matches the URL filter named **MyFilter**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ip urlfilter MyFilter in**

ipv6 dhcp relay destination *<ipv6 address>*

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination *<ipv6 address>*
ipv6 dhcp relay destination *<ipv6 address> <interface>*

Syntax Description

<ipv6 address>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** *<ipv6 address>* **?** to display a list of valid interfaces.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the Tunnel interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command **ipv6**.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#ipv6**
(config-hdlc 1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

keepalive <*value*>

Use the **keepalive** command to enable the transmission of keepalive packets on the interface and specify the time interval in seconds between transmitted packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Defines the time interval (in seconds) between transmitted keepalive packets. Valid range is **0** to **32767** seconds.

Default Values

By default, the time interval between transmitted keepalive packets is **10** seconds.

Command History

Release 9.1	Command was introduced.

Functional Notes

If three keepalive packets are sent to an interface with no response, the interface is considered down. To detect interface failures quickly, specify a smaller keepalive time.

Usage Examples

The following example specifies a keepalive time of 5 seconds on the high level data link control (HDLC) interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#keepalive 5**

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the high level data link control (HDLC) interface to receive LLDP packets:

(config)**#interface hdlc 1**
(config-hdlc 1)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to disable this feature. Variations of this command include:

lldp send
lldp send management-address
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

By default, all interfaces are configured to transmit and receive LLDP packets of all types.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the high level data link control (HDLC) interface to transmit LLDP packets containing all enabled information types:

(config)**#interface hdlc 1**
(config-hdlc 1)**#lldp send**

The following example configures the HDLC to transmit and receive LLDP packets containing all information types:

(config)**#interface hdlc 1**
(config-hdlc 1)**#lldp send-and-receive**

max-reserved-bandwidth <*value*>

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<*value*>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies **85** percent of the bandwidth on the high level data link control (HDLC) 1 be available for use in user-defined queues:

(config)**#interface hdlc 1**
(config-hdlc 1)**#max-reserved-bandwidth 85**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip secondary <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A4.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface hdlc 1**
(config-hdlc 1)**#media-gateway ip primary**

packet-capture <*name*>

Use the **packet-capture** command to apply a previously configured packet capture instance to the interface. Use the **no** form of this command to remove the packet capture instance.

Syntax Description

<*name*>	Specifies the name of the packet capture instance to apply to the interface.

Default Values

By default, no packet capture instances are configured or applied to the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. For more information about packet capturing, its uses, and its implementation in AOS, refer to the configuration guide *Configuring Packet Capture in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example applies the previously configured packet capture **1CAPTURE** to the interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#packet-capture 1CAPTURE**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing (WFQ).
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the high level data link control (HDLC) interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the high level data link control (HDLC) interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#rtp quality-monitoring**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example disables the link-status trap on the HDLC interface:

(config)**#interface hdlc 1**
(config-hdlc 1)**#no snmp trap link-status**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the HDLC interface to the VRF instance named **RED**:

(config)**#interface hdlc 1**
(config-hdlc 1)**#vrf forwarding RED**

LOOPBACK INTERFACE COMMAND SET

To create a virtual loopback interface and/or activate the Loopback Interface Configuration mode, enter the **interface loopback** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface loopback 1
(config-loop 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bandwidth <value> on page 2969
dynamic-dns on page 2970
ip commands begin on page 2972
ipv6 commands begin on page 3009
ospfv3 <process id> area <area id> on page 3027
ospfv3 <process id> shutdown on page 3029
rtp quality-monitoring on page 3030
snmp trap on page 3031
snmp trap link-status on page 3032
vrf forwarding <name> on page 3033

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view the default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.

Functional Notes

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface.

Usage Examples

The following example sets bandwidth of the loopback interface to 10 Mbps:

(config)**#interface loopback 1**
(config-loop 1)**#bandwidth 10000**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface loopback 1**
(config-loop 1)**#dynamic-dns dyndns-custom host user pass**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to create an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Specifies IPv4 ACL name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to allow only Telnet traffic into the loopback interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface loopback 1**
(config-loop 1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the loopback interface 1:

(config)**#interface loopback 1**
(config-loop 1)**#ip access-policy PRIVATE**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 2.1	Added **ip address dhcp** for Dynamic Host Configuration Protocol (DHCP) client support.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 255.255.255.252**:

(config)**#interface loopback 1**
(config-loop 1)**#ip address 192.22.72.101 255.255.255.252 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface loopback 1**
(config-loop 1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

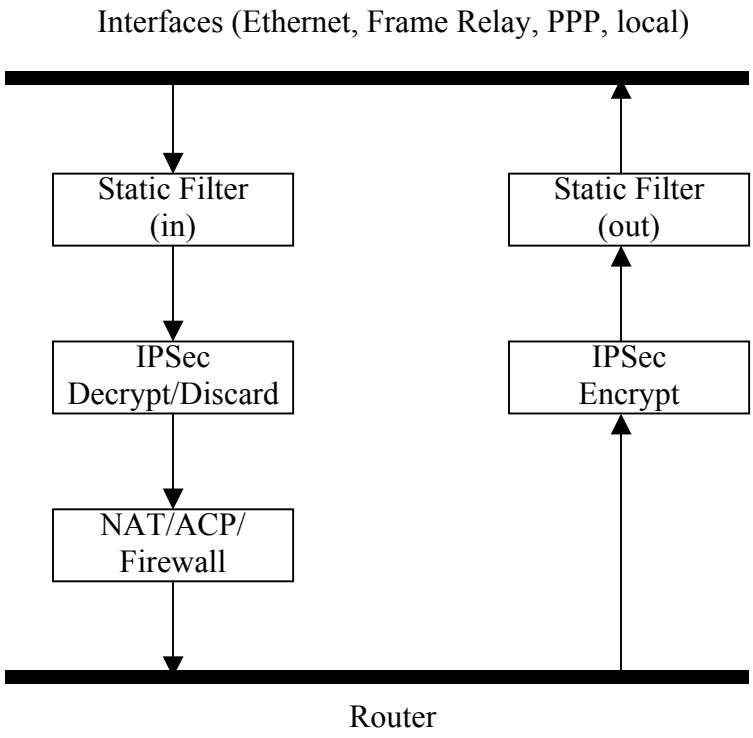
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip crypto map MyMap**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface loopback 1**
(config-loop 1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **loopback 1**:

(config)**#interface loopback 1**
(config-loop 1)**#ip directed-broadcast**

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on a **loopback** interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface loopback 1**
(config-loop 1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper-address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248 /30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface loopback 1**
(config-loop 1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface loopback 1**
(config-loop 1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 2990* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip mcast-stub downstream**

ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*ip address*> command to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include the loopback interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 2987*, and *ip mcast-stub upstream on page 2990* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface loopback 1**
(config-loop 1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 2987* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

```
(config)#interface loopback 1
(config-loop 1)#ip mcast-stub upstream
```


ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip mtu 1200**

ip ospf <*process id*> area <*area id*>

Use the **ip ospf area** command to add an interface to an Open Shortest Path First version 2 (OSPFv2) process, and to configure the OSPFv2 process on the interface. This command places the interface in the specified area. Use the **no** form of this command to remove the OSPFv2 process from the interface.

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.

iDefault Values

By default, an OSPFv2 process is not configured on an interface. By default, process IDs and area IDs.

Command History

Release R11.3.0	Command was introduced.

Usage Examples

To add an interface to the OSPFv2 process **5** in area **10**:

(config)**#interface loopback 1**
(config-loop 1)**#ip ospf 5 area 10**

ip ospf <*process id*> shutdown

Use the **ip ospf shutdown** command to disable an Open Shortest Path First version 2 (OSPFv2) process on the interface. When this command is used, the OSPFv2 setting remain in place, but logically it appears to the interface as though the OSPFv2 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv2 process.

Syntax Description

<process id>	Specifies the OSPFv2 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ip ospf <process id> area <area id> on page 2993*), entering this command will not create the ID. Only one OSPFv2 process can be configured at a time; if another OSPFv2 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R11.3.0	Command was introduced.

Usage Examples

The following example disables OSPFv2 process **5** on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip ospf 5 shutdown**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the loopback 1 interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the loopback 1 interface every **3600** seconds:

(config)**#interface loopback 1**
(config-loop 1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the PIM sparse neighbor timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to 300 seconds:

(config)**#interface loopback 1**
(config-loop 1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface loopback 1**
(config-loop 1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation delay to **300** milliseconds:

(config)**#interface loopback 1**
(config-loop 1)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the loopback interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the loopback interface to accept only RIP version 2 packets:

(config)**#interface loopback 1**
(config-loop 1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP **version 1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip send version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the loopback interface to transmit only RIP version 2 packets:

(config)**#interface loopback 1**
(config-loop 1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface loopback 1**
(config-loop 1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route-cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the loopback interface:

(config)**#interface loopback 1**
(config-loop 1)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a complete list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered ppp 1** while in the Ethernet Interface Configuration mode configures the Ethernet interface to use the IP address assigned to the Point-to-Point Protocol (PPP) interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the loopback interface (labeled **loop 1**) to use the IP address assigned to the PPP interface (**ppp 1**):

(config)**#interface loopback 1**
(config-loop 1)**#ip unnumbered ppp 1**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the loopback interface (labeled **loop 1**) and matches the URL filter named **MyFilter**:

(config)**#interface loopback 1**
(config-loop 1)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on an interface. Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the interface.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the interface.

Command History

Release 18.1	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the interface to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the interface.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an interface when other unicast IPv6 addresses are not needed on the interface. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the interface.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6**

ipv6 access-policy *<ipv6 acp name>*

Use the **ipv6 access-policy** command to assign a specified Internet Protocol version 6 (IPv6) access control policy (ACP) to an interface. IPv6 ACPs are applied to IPv6 traffic entering an interface. Use the **no** form of this command to remove an ACP association.

Syntax Description

<ipv6 acp name>	Identifies the configured IPv6 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv6 ACPs associated with an interface.

Command History

Release 18.1	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.

Usage Examples

The following example applies the IPv6 ACP **PRIVATEv6** to the interface:

Enable the AOS security features:
(config)**#ipv6 firewall**

Associate the ACP with the PPP interface:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 access-policy PRIVATEv6**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3013*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3013*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the interface and enables IPv6 processing on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address <*ipv6 link-local address*> link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<*ipv6 link-local address*>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the interface.

Default Values

By default, no IPv6 address is configured for the interface and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.

Functional Notes

A single link-local address can be manually configured on an interface. The lower 64 bits of the specified address become the Interface ID for the interface, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the interface and can be derived from the interface's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the interface.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example manually creates a link-local IPv6 address on the interface and enables IPv6 processing:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname <*partial fqdn*>
ipv6 address dhcp hostname fqdn <*fqdn*>
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 3009*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 address 2001:DB8:1::1/64**
(config-loop 1)**#ipv6 address dhcp fqdn client@company.com**

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*

Use the **ipv6 address named-prefix** command to create an Internet Protocol version 6 (IPv6) address for the interface using the values in a named prefix. Use the **no** form of this command to remove the address from the interface. Variations of this command include:

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*
ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>* **eui-64**

Syntax Description

<prefix name>	Specifies the named prefix to use to create the address.
<ipv6 address/prefix-length>	Specifies the address portion appended to the named prefix to create a 128-bit host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
eui-64	Optional. Indicates that the interface ID is to be placed in the lower 64 bits of the address.

Default Values

By default, no IPv6 addresses are specified on the interface.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example creates an IPv6 address on the interface using the named prefix **PREFIX1**:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 address named-prefix PREFIX1 2001:1:0:/48**

ipv6 dhcp client information refresh minimum <*seconds*>

Use the **ipv6 dhcp client information refresh minimum** command to specify the minimum value the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the interface accepts as its information refresh timer. Use the **no** version of this command to return to the default setting.

Syntax Description

<*seconds*>	Specifies the refresh timer in seconds. Valid range is **600** to **3600** seconds.

Default Values

By default, the DHCPv6 client refresh timer is set to **600** seconds.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example specifies the DHCPv6 client refresh timer for the interface is **800** seconds:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 dhcp client information refresh minimum 800**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 dhcp client pd PREFIX1**

ipv6 dhcp relay destination <*ipv6 address*>

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination <*ipv6 address*>
ipv6 dhcp relay destination <*ipv6 address*> <*interface*>
ipv6 dhcp relay destination <*ipv6 address*> **mef-ethernet** <*slot/port*>
ipv6 dhcp relay destination <*ipv6 address*> **system-control-evc**
ipv6 dhcp relay destination <*ipv6 address*> **system-management-evc**

Syntax Description

<*ipv6 address*>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*interface*>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** <*ipv6 address*> **?** to display a list of valid interfaces.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC) is used when sending messages to the DHCPv6 server.
system-management-evc	Optional. Specifies the system management EVC is used when sending messages to the DHCPv6 server.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command *ipv6 on page 3009*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6**
(config-loop 1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped mulitcast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the interface and specify that the interface is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the interface, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the interface. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this interface. All DHCPV^ requests received on this interface are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the interface.

Command History

Release R10.1.0	Command was introduced.
Release R10.5.0	Command was expanded to include the loopback interface.

Functional Notes

Enabling the interface as a DHCPv6 server using this command places the interface into DHCPv6 server mode. DHCPv6 modes (server or relay) are mutually exclusive at the interface. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the interface as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 address 2001:DB8:1::1/64**
(config-loop 1)**#ipv6 dhcp server POOL1**

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the interface in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the interface.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the interface in host mode:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 mode host unicast**

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the interface. Use the **no** form of this command to remove the specified prefix configuration from the interface. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the interface is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the interface. Prefixes for IPv6 addresses configured on a router interface are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the interface.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#interface loopback 1**
(config-loop 1)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ospfv3 <*process id*> **area** <*area id*>

Use the **ospfv3 area** command to add an interface to an Open Shortest Path First version 3 (OSPFv3) process, and to configure the OSPFv3 process on the interface. This command places the interface in the specified area for the specified Internet Protocol version 6 (IPv6) OSPFv3 address family, and optionally defines the instance ID that is used to represent this OSPFv3 process in messages on the interface's link. Use the **no** form of this command to remove the OSPFv3 process from the interface. Variations of this command include:

ospfv3 <*process id*> **area** <*area id*> **ipv6**
ospfv3 <*process id*> **area** <*area id*> **ipv6 instance** <*instance id*>

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join, for the specified address family. The process ID is locally significant to the device, and must be unique among all OSPFv3 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the given OSPFv3 process. Valid range is **0** to **4294967295**.
ipv6	Identifies the OSPFv3 address family as IPv6.
instance <*instance id*>	Optional. Specifies the value to use in the instance ID field of messages sent or received by this OSPFv3 process on the interface's link. Valid range is **0** to **31**.

Default Values

By default, an OSPFv3 process is not configured on an interface. By default, process IDs, area IDs, and instance IDs are not defined.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

When using this command to enable an OSPFv3 process on an interface, keep the following rules in mind:

- The interface must have the address family enabled on the interface. If the address family is not enabled on the interface, the command is rejected and an error is displayed.
- Only interfaces on the default virtual routing and forwarding (VRF) instance support this command. Interfaces on a nondefault VRF will display an error when you attempt to configure OSPFv3 settings.
- The interface and the specified OSPFv3 process (if defined in the global configuration) must be in the same VRF or the command will fail.
- The address family must match that specified for the OSPFv3 process if the process has been defined in the global configuration or the command will fail.
- If the OSPFv3 process identified by the process ID does not exist in the global configuration, it is automatically created, along with the specified address family, and it is assigned to the VRF of which the interface is a member.

- If the specified OSPFv3 process is already at its maximum limit of processes or address families, the command fails.
- If the specified OSPFv3 process already exists in the global configuration, but its configuration does not include an address family, the specified address family is added to the OSPFv3 router configuration.
- A given OSPFv3 process can only have one address family.
- Multiple OSPFv3 instances per address family, per VRF, can be created and can be assigned to a given interface.
- If the interface's VRF changes, all OSPFv3 assignments are removed.
- To change an OSPFv3 process's VRF, the process must first be removed and then recreated. Removing the process removes all OSPFv3 assignments for that process form all interfaces.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To add an interface to the OSPFv3 process **5**, in area **10**, with an instance ID of **10**, enter the command as follows:

(config)**#interface loopback 1**
(config-loop 1)**#ospfv3 5 area 10 ipv6 instance 10**

ospfv3 <*process id*> shutdown

Use the **ospfv3 shutdown** command to disable an Open Shortest Path First version 3 (OSPFv3) process on the interface. When this command is used, the OSPFv3 commands remain in place, but logically it appears to the interface as though the OSPFv3 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv3 process.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3027*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables OSPFv3 process **5** on the interface:

(config)**#interface loopback 1**
(config-loop 1)**#ospfv3 5 shutdown**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the loopback interface:

(config)**#interface loopback 1**
(config-loop 1)**#rtp quality-monitoring**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP capability on the loopback interface:

(config)**#interface loopback 1**
(config-loop 1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI)
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.2	Command was expanded to the cellular interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the loopback interface:

(config)**#interface loopback 1**
(config-loop 1)**#no snmp trap link-status**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the loopback interface to the VRF instance named **RED**:

(config)**#interface loopback 1**
(config-loop 1)**#vrf forwarding RED**

PORT CHANNEL INTERFACE COMMAND SET

To create a virtual link aggregation interface and/or activate the Port Channel Interface Configuration mode, enter the **interface port-channel** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface port-channel 1
(config-p-chan1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

arp arpa on page 3035
lldp receive on page 3036
lldp send on page 3037
qos on page 3039
snmp trap on page 3040
snmp trap link-status on page 3041
spanning tree commands begin on page 3042
storm-control action shutdown on page 3048
storm-control level on page 3049
storm-control rate on page 3051
switchport commands begin on page 3053

arp arpa

Use the **arp arpa** command to set ARPA as the standard Address Resolution Protocol (ARP) on this interface. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

The default for this command is **arpa**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables standard ARP for the port channel interface:

```
(config)#interface port-channel 1
(config-p-chan1)#arp arpa
```

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the port channel interface to receive LLDP packets:

(config)**#interface port-channel 1**
(config-p-chan1)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to disable this feature. Variations of this command include:

lldp send management-address
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

By default, all interfaces are configured to transmit and receive LLDP packets of all types.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the port channel interface to transmit LLDP packets containing all enabled information types:

(config)**#interface port-channel 1**
(config-p-chan1)**#lldp send**

The following example configures the port channel interface to transmit and receive LLDP packets containing all information types:

(config)**#interface port-channel 1**
(config-p-chan1)**#lldp send-and-receive**

qos

Use the **qos** command to set the interface to the trusted state and to set the default class of service (CoS) value. Use the **no** form of this command to return to the default setting. Variations of this command include:

qos default-cos <*value*>
qos trust cos

Syntax Description

default-cos <*value*>	Sets the default CoS value for untrusted ports and all untagged packets. Range is **0** to **7**.
trust cos	Sets the interface to the trusted state.

Default Values

By default, the interface is untrusted with a default CoS of **0**.

Command History

Release 5.1	Command was introduced.

Functional Notes

Set the interface to **trust cos** if received 802.1P. CoS values are considered valid (i.e., no need to reclassify) and do not need to be tagged with the default value. When set to untrusted, the **default-cos** value for the interface is used.

Usage Examples

The following example sets port channel 1 as a trusted interface and assigns untagged packets a CoS value of 1:

(config)**#interface port-channel 1**
(config-p-chan1)**#qos trust cos**
(config-p-chan1)**#qos default-cos 1**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP capability on the port channel interface:

(config)**#interface port-channel 1**
(config-p-chan1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.2	Command was expanded to the cellular interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the port channel interface:

(config)**#interface port-channel 1**
(config-p-chan1)**#no snmp trap link-status**

spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** command to enable or disable the bridge protocol data unit (BPDU) filter on a specific interface. This setting overrides the related global setting (refer to *spanning-tree edgeport default on page 1837*). Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree bpdufilter disable
spanning-tree bpdufilter enable

Syntax Description

disable	Disables BPDU filter for this interface.
enable	Enables BPDU filter for this interface.

Default Values

By default, this setting is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpdufilter blocks any BPDUs from being transmitted and received on an interface.

Usage Examples

The following example enables the BPDU filter on the port channel interface:

(config)**#interface port-channel 3**
(config-p-chan3)**#spanning-tree bpdufilter enable**

The BPDU filter can be disabled on port channel 3 by issuing the following commands:

(config)**#interface port-channel 3**
(config-p-chan3)**#spanning-tree bpdufilter disable**

spanning-tree bpduguard

Use the **spanning-tree bpduguard** command to enable or disable the bridge protocol data unit (BPDU) guard on a specific interface. This setting overrides the related global setting (refer to *spanning-tree edgeport default on page 1837*). Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree bpduguard disable
spanning-tree bpduguard enable

Syntax Description

disable	Disables BPDU guard for this interface.
enable	Enables BPDU guard for this interface.

Default Values

By default, this setting is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpduguard blocks any BPDUs from being received on an interface.

Usage Examples

The following example enables the BPDU guard on the port channel interface:

(config)**#interface port-channel 3**
(config-p-chan3)**#spanning-tree bpduguard enable**

The BPDU guard can be disabled on port channel 3 by issuing the following commands:

(config)**#interface port-channel 3**
(config-p-chan3)**#spanning-tree bpduguard disable**

spanning-tree cost <*value*>

Use the **spanning-tree cost** command to assign a cost to the interface. The cost value is used when computing the spanning-tree root path. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies a cost value of **1** to **200000000**.

Default Values

By default, the cost value is set to **1000**/(link speed in Mbps).

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the interface to a path cost of **1200**:

(config)**#interface port-channel 3**
(config-p-chan3)**#spanning-tree cost 1200**

spanning-tree edgeport

Use the **spanning-tree edgeport** command to configure the interface to be an edgeport. This command overrides the global setting (refer to *spanning-tree edgeport default on page 1837*). Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this setting is disabled.

Command History

Release 5.1	Command was introduced.
Release 8.1	Command was added to the ATM Subinterface command set.

Functional Notes

When an interface is designated as an edgeport, the interface will immediately go to a forwarding state when the link becomes active. When an interface is not designated as an edgeport, the interface must go through the listening and learning states before going to the forwarding state.

Usage Examples

The following example configures the interface to be an edgeport:

(config)**#interface port-channel 1**
(config-p-chan1)**#spanning-tree edgeport**

An individual interface can be configured to not be considered an edgeport. For example:

(config)**#interface port-channel 1**
(config-p-chan1)**#spanning-tree edgeport disable**

or

(config)**#interface port-channel 1**
(config-p-chan1)**#no spanning-tree edgeport**

spanning-tree link-type

Use the **spanning-tree link-type** command to configure the spanning tree protocol link type for each interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared

Syntax Description

auto	Determines link type by the port's duplex settings.
point-to-point	Manually sets link type to point-to-point regardless of duplex settings.
shared	Manually sets link type to shared regardless of duplex settings.

Default Values

By default, the interface is set to **auto**.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command overrides the default link type setting determined by the duplex of the individual port. By default, a port configured for half-duplex is set to **shared** link type, and a port configured for full-duplex is set to **point-to-point** link type. Setting the link type manually overrides the default and forces the port to use the specified link type. Use the **link-type auto** command to restore the convention of determining link type based on duplex settings.

Usage Examples

The following example forces the link type to **point-to-point**, even if the port is configured to be half-duplex:

(config)**#interface port-channel 1**
(config-p-chan1)**#spanning-tree link-type point-to-point**

Technology Review

Rapid transitions are possible in Rapid Spanning Tree Protocol (RSTP) by taking advantage of point-to-point links (a port is connected to exactly one other bridge) and edge-port connections (a port is not connected to any additional bridges). Setting the link type to **point-to-point** allows a half-duplex link to act as if it were a point-to-point link.

spanning-tree port-priority <*value*>

Use the **spanning-tree port-priority** command to select the priority level of this interface. To return to the default setting, use the **no** form of this command.

Syntax Description

<*value*>	Specifies a priority-level value from **0** to **240** (this value must be in increments of 16).

Default Values

By default, the **spanning-tree port-priority** is set to **128**.

Command History

Release 5.1	Command was introduced.

Functional Notes

The only time that this priority level is used is when two interfaces with a path to the root have equal cost. At that point, the level set in this command will determine which port the spanning tree will use. Set the priority value lower to increase the chance the interface will be used.

Usage Examples

The following example sets the interface to a priority of **96**:

(config)**#interface port-channel 4**
(config-p-chan4)**#spanning-tree port-priority 96**

storm-control action shutdown

Use the **storm-control action shutdown** command to specify that the unit should shutdown when a broadcast, multicast, or unicast storm occurs. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled; the interface will only filter traffic.

Command History

Release 5.1	Command was introduced.

Functional Notes

Enabling this option shuts down the interface if a multicast, unicast, or broadcast storm occurs.

Usage Examples

The following example shuts down the port channel interface if a storm is detected:

(config)**#interface port-channel 1**
(config-p-chan1)**#storm-control action shutdown**

storm-control level

Use the **storm-control level** command to configure limits on the rates of broadcast, multicast, and unicast traffic on a port. Use the **no** form of this command to disable this feature. Variations of this command include:

storm-control broadcast level *<rising level>*
storm-control broadcast level *<rising level> <falling level>*
storm-control multicast level *<rising level>*
storm-control multicast level *<rising level> <falling level>*
storm-control unicast level *<rising level>*
storm-control unicast level *<rising level> <falling level>*

Syntax Description

broadcast level	Sets levels for broadcast traffic.
multicast level	Sets levels for multicast traffic.
unicast level	Sets levels for unicast traffic.
<rising level>	Specifies a rising level which determines the percentage of total bandwidth the port accepts before it begins blocking packets. Range is **1** to **100** percent.
<falling level>	Optional. Specifies a falling level which determines when the storm is considered over, causing AOS to no longer block packets. This level must be less than the rising level. Range is **1** to **100** percent.

Default Values

By default, **storm-control** is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

This setting configures the rising and falling suppression values. When the selected rising level (which is a percentage of total bandwidth) is reached, the port begins blocking packets of the specified type (i.e., broadcast, multicast, or unicast). AOS uses the rising level as its falling level if no falling level is specified.

Usage Examples

The following example sets the rising suppression level to **85** percent for multicast packets:

(config)**#interface port-channel 1**
(config-p-chan1)**#storm-control multicast level 85**

The following example sets the rising suppression level to **80** percent for broadcast packets, with a falling level of **50** percent:

(config)**#interface port-channel 1**
(config-p-chan1)**#storm-control broadcast level 80 50**

storm-control rate

Use the **storm-control rate** command to configure maximum ingress data rates for broadcast, unknown multicast, and unknown unicast traffic on a switch port. Use the **no** form of this command to disable the feature. Variations of this command include:

storm-control broadcast rate <*rate*>
storm-control broadcast rate <*rate*> **burst** <*size*>
storm-control multicast-unknown rate <*rate*>
storm-control multicast-unknown rate <*rate*> **burst** <*size*>
storm-control unicast-unknown rate <*rate*>
storm-control unicast-unknown rate <*rate*> **burst** <*size*>

Syntax Description

broadcast	Specifies the maximum data rate for all ingress broadcast traffic.
multicast-unknown	Specifies the maximum data rate for ingress unknown multicast traffic.
unicast-unknown	Specifies the maximum data rate for ingress unknown unicast traffic.
rate <*rate*>	Specifies the maximum ingress data rate in Kilobytes per second. Valid range is **64** to **33554368** Kbps.
burst <*size*>	Optional. Specifies the maximum traffic burst (in bytes) of the specified traffic type that can ingress the port. Valid selections are **4K**, **16K**, **64K**, **256K**, **1M**, **4M**, **8M**, and **16M** bytes.

Default Values

By default, storm control is disabled. When enabled, the burst size is set to **64K** bytes by default.

Command History

Release R11.8.0	Command was introduced.

Functional Notes

Storm control is used to lessen the impacts of traffic flooding on certain ports.

Address Resolution Protocol (ARP), Dynamic Host Control Protocol (DHCP), and other protocols commonly use broadcasts, so setting the broadcast storm control rate too low can adversely impact these protocols in an otherwise healthy network.

The configured multicast storm control rate applies only to multicast traffic with addresses not learned by Internet Group Management Protocol (IGMP) snooping.

Unknown unicast traffic usually exist only for initial traffic to a client or traffic sent to a client that was unlearned or that timed out. Setting the unicast storm control rate too low can impact traffic to clients that actually exist but are temporarily unknown to the switch. Spanning tree topology change notifications (TCNs) clear the known unicast addresses on some ports of the switch and cause all unicast traffic from these clients to be unknown until the addresses are relearned. This behavior can cause the temporary rate of unknown unicast frames to spike. Switching networks that have relatively static topologies should use the spanning tree edge-port setting to limit spanning tree TCNs so that a lower storm control unicast rate can be set. If the network topology changes frequently, a larger unicast storm control rate should be set so that traffic is not adversely impacted after a spanning tree TCN.

All traffic is received on switchports at full line rate, meaning that the momentary rate of received traffic will almost always exceed any storm control rate configured lower than the port's linked rate. The configured burst size determines how many bytes can burst over the configured rate before storm control makes a decision to begin dropping traffic for a configured traffic type. A smaller storm control burst size causes the rate to be imposed on received frames earlier in the storm of undesired frames. Setting a higher burst rate is less likely to drop frames in case of many back-to-back frames, but also exposes the network to more of the initial frames of a storm of undesired frames. Once a burst is exhausted, it takes an interval of time to refill completely. This interval, in seconds, is defined as the (burst rate * 8)/rate.

When a switchport is part of a port channel, storm control settings are not allowed on the switchport. Rather, storm control rate and burst settings are only allowed on the port channel of which the switchport is a member.

Usage Examples

The following example configures broadcast traffic storm control with a rate of **1000** Kbps and the default burst size:

(config)**#interface port-channel 1**
(config-p-chan1)**#storm-control broadcast rate 1000**

switchport access vlan *<vlan id>*

Use the **switchport access vlan** command to set the port to be a member of the virtual local area network (VLAN) when in access mode. To reset the port to be a member of the default VLAN, use the **no** form of this command.

Syntax Description

<vlan id>	Specifies a valid VLAN interface ID. Range is **1** to **4094**.

Default Values

By default, this is set to VLAN 1 (the default VLAN).

Command History

Release 5.1	Command was introduced.

Functional Notes

If the port is in the trunk mode, this command will not alter the switchport mode to access. Instead, it will save the value to be applied when the port does switch to access mode. Refer to *switchport mode on page 3055* for more information.

Usage Examples

The following example sets the switchport mode to static access, and makes the port channel 1 a member of VLAN 2:

(config)**#interface port-channel 1**
(config-p-chan1)**#switchport mode access**
(config-p-chan1)**#switchport access vlan 2**

switchport gvrp

Use the **switchport gvrp** command to enable GARP VLAN Registration Protocol (GVRP) on an interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, GVRP is disabled on all ports.

Command History

Release 8.1	Command was introduced.

Functional Notes

Enabling GVRP on any interface enables GVRP globally.

Usage Examples

The following example enables GVRP on port channel 3:

```
(config)#interface port-channel 3
(config-p-chan3)#switchport gvrp
```

switchport mode

Use the **switchport mode** command to configure the virtual local area network (VLAN) membership mode. Use the **no** form of this command to reset membership mode to the default value. Variations of this command include:

switchport mode access
switchport mode trunk

Syntax Description

access	Sets port to be a single (nontrunked) port that transmits and receives no tagged packets.
trunk	Sets port to transmit and receive packets on all VLANs included within its VLAN allowed list.

Default Values

By default, this is set to **access**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the port to be a trunk port:

(config)**#interface port-channel 1**
(config-p-chan1)**#switchport mode trunk**

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** command to allow certain virtual local area networks (VLANs) to transmit and receive traffic on this port when the interface is in trunking mode. To return to the default setting, use the **no** form of this command. Variations of this command include:

switchport trunk allowed vlan <*list*>
switchport trunk allowed vlan add <*list*>
switchport trunk allowed vlan all
switchport trunk allowed vlan except <*list*>
switchport trunk allowed vlan remove <*list*>

Syntax Description

add	Adds the specified VLAN IDs to the VLAN trunking allowed list.
all	Adds all configured VLAN IDs to the VLAN trunking allowed list.
except	Adds all configured VLAN IDs to the VLAN trunking allowed list except those specified in the VLAN ID list.
remove	Removes VLAN IDs from the VLAN trunking allowed list.
<*list*>	Specifies a list of valid VLAN interface IDs. Refer to *Functional Notes* below for additional syntax considerations.

Default Values

By default, all valid VLANs are allowed.

Command History

Release 5.1	Command was introduced.

Functional Notes

A VLAN list is a set of VLAN IDs. A valid VLAN ID value must be from 1 to 4094 (inclusive). Each VLAN ID in a list is delimited by commas, yet a range of IDs may be expressed as a single element by using a hyphen between endpoints. For example, the VLAN ID range **1,2,3,4,6,7,8,9,500** may be more easily expressed as **1-4,6-9,500**. No spaces are allowed in a valid ID range.

Usage Examples

The following example adds VLANs to the previously existing list of VLANs allowed to transmit and receive on this port:

(config)**#interface port-channel 1**
(config-p-chan1)**#switchport trunk allowed vlan add 1-4,6-9,500**

switchport trunk fixed vlan

Use the **switchport trunk fixed vlan** command to change the configured list of virtual local area networks (VLANs) that remain fixed in use only when GARP VLAN Registration Protocol (GVRP) is enabled on the interface. Of these VLANs, VLANs statically or dynamically created will be available for use on the interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

switchport trunk fixed vlan *<list>*
switchport trunk fixed vlan add *<list>*
switchport trunk fixed vlan all
switchport trunk fixed vlan except *<list>*
switchport trunk fixed vlan none
switchport trunk fixed vlan remove *<list>*

Syntax Description

add	Adds VLANs to the VLAN GVRP trunking fixed list.
all	Adds all VLANs to the VLAN GVRP trunking fixed list.
except	Adds all VLAN IDs to the VLAN trunking fixed list except those in the command line VLAN ID list.
none	Removes all VLANs from the VLAN GVRP trunking fixed list.
remove	Removes VLAN from the VLAN trunking fixed list.
<list>	Specifies a list of valid VLAN interface IDs. Refer to *Functional Notes* below for additional syntax considerations.

Default Values

By default, no VLANs are in the VLAN GVRP trunking fixed list (**switchport trunk fixed vlan none**).

Command History

Release 8.1	Command was introduced.

Functional Notes

This command has no effect on VLAN membership configuration unless GVRP is enabled on the interface. Refer to *gvrp on page 1312* for information on enabling GVRP.

A VLAN list is a set of VLAN IDs. A valid VLAN ID value must be from 1 to 4094 (inclusive). Each VLAN ID in a list is delimited by commas, yet a range of IDs may be expressed as a single element by using a hyphen between endpoints. For example, the VLAN ID range **1,2,3,4,6,7,8,9,500** may be more easily expressed as **1-4,6-9,500**. No spaces are allowed in a valid ID range.

Usage Examples

The following example changes the configured list of fixed VLANs by adding VLAN 50 to the list:

(config-p-chan1)**#switchport trunk fixed vlan add 1-15,25-30,40**
(config-p-chan1)#
(config-p-chan1)**#switchport trunk fixed vlan add 50**
(config-p-chan1)#

switchport trunk native vlan <*vlan id*>

Use the **switchport trunk native vlan** command to set the virtual local area network (VLAN) native to the interface when the interface is in trunking mode. To return to defaults, use the **no** form of this command.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Range is **1** to **4094**.

Default Values

By default, **switchport trunk native vlan** is set to VLAN 1.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configure which VLAN the interface uses as its native VLAN during trunking. Packets from this VLAN leaving the interface will not be tagged with the VLAN number. Any untagged packets received by the interface are considered a part of the native VLAN ID.

Usage Examples

The following example sets the native VLAN on port channel 1 to VLAN 2:

(config)**#interface port-channel 1**
(config-p-chan1)**#switchport trunk native vlan 2**

PPP INTERFACE COMMAND SET

To create a virtual Point-to-Point Protocol (PPP) interface and/or activate the PPP Interface Configuration mode, enter the **interface ppp** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface ppp 1
(config-ppp 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

acfc accept-compressed on page 3062
alias link "<text>" on page 3063
bandwidth <value> on page 3064
bridge-group commands begin on page 3065
dial-backup commands begin on page 3067
dynamic-dns on page 3083
fair-queue on page 3085
hold-queue <value> out on page 3086
ip commands begin on page 3087
ipv6 commands begin on page 3132
keepalive <value> on page 3168
lldp receive on page 3169
lldp send on page 3170
max-reserved-bandwidth <value> on page 3172
media-gateway ip on page 3173
media-gateway ipv6 on page 3175
ospfv3 commands begin on page 3177
peer default ip address <ipv4 address> on page 3190
peer default ipv6 interface-id <interface id> on page 3191

acfc accept-compressed

Use the **acfc accept-compressed** command to enable accepting header compressed frames even if compression is not negotiated. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example enables accepting compressed frames:

(config)**#interface ppp 1**
(config-ppp 1)**#acfc accept-compressed**

alias link “*<text>*”

Use the **alias link** command to provide the management station with an identifying description for each link (Point-to-Point Protocol (PPP) physical). Each configured PPP interface (when referenced using Simple Network Management Protocol (SNMP)) contains a link (physical port) and a bundle (group of links). RFC 1471 (for Link Connection Protocol) provides an interface table to manage lists of bundles and associated links. Use the **no** form of this command to return to the default setting.

Syntax Description

“<text>”	Describes the interface (for SNMP) by alphanumeric character string (must be encased in quotation marks).

Default Values

By default, the PPP identification string appears as empty quotation marks (“ ”).

Command History

Release 1.1	Command was introduced.

Functional Notes

The **alias link** string should be used to uniquely identify a PPP link. Enter a string that clearly identifies the link.

Usage Examples

The following example defines a unique character string for the virtual PPP interface (1):

(config)**#interface ppp 1**
(config-ppp 1)**#alias link “PPP_link_1”**

Technology Review

Please refer to RFC 1990 for a more detailed discussion on PPP links and bundles.

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies the bandwidth value in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view the default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 3172*) to adjust the bandwidth appropriately for QoS configurations.

Usage Examples

The following example sets bandwidth of the Point-to-Point Protocol (PPP) interface to 10 Mbps:

(config)**#interface ppp 1**
(config-ppp 1)**#bandwidth 10000**

bridge-group *<number>*

Use the **bridge-group** command to assign an interface to the specified bridge group. This command is supported on all Ethernet interfaces, Point-to-Point Protocol (PPP) virtual interfaces, and Frame Relay virtual subinterfaces. Use the no form of this command to remove an interface.

Syntax Description

<number>	Specifies the bridge group (by number) to which to assign this interface. Range is **1** to **255**.

Default Values

By default, there are no configured bridge groups.

Command History

Release 1.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (Ethernet to T1 bridge, Ethernet to Frame Relay subinterface, etc.).

Usage Examples

The following example assigns the PPP interface to **bridge-group 1**:

(config)**#interface ppp 1**
(config-ppp 1)**#bridge-group 1**

bridge-group <*number*> vlan-transparent

Use the **bridge-group vlan-transparent** command to prevent an interface from removing the virtual local area network (VLAN) tag. Use the **no** form of this command to allow the interface to remove the VLAN tag from the packet.

*The **bridge-group vlan-transparent** command is not a global command. The command must be applied on all interfaces of the bridge group.*

Syntax Description

<number>	Specifies the bridge group number. Valid range is **1** to **255**.

Default Values

By default, VLAN tags are removed from the data.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the high level data link control (HDLC) interface and Frame Relay subinterface.

Usage Examples

The following example prevents the removal of VLAN tags from the packets on the Point-to-Point Protocol (PPP) interface labeled 1:

(config)**#interface ppp 1**
(config-ppp 1)**#bridge-group 1 vlan-transparent**

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the interface to automatically attempt a dial backup upon failure. Use the **no** form of this command to disable this feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3070*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial backup upon a failure.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example enables automatic dial backup on the endpoint:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup auto-backup**

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3070*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to automatically restore the primary connection when the failure condition clears:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup auto-restore**

dial-backup backup-delay *<value>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3070*.

Syntax Description

<value>	Specifies the delay period (in seconds) a failure must be active before AOS will enter backup operation on the interface. Range is **10** to **86400** seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **60** seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup backup-delay 60**

dial-backup call-mode

Use the **dial-backup call-mode** command to specify whether the configured backup interface answers or originates (or a combination of both) backup calls. Use the **no** form of this command to return to the default value. Variations of this command include:

dial-backup call-mode answer
dial-backup call-mode answer-always
dial-backup call-mode originate
dial-backup call-mode originate-answer
dial-backup call-mode originate-answer-always

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer**.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Functional Notes

The majority of the configuration for AOS dial-backup implementation is configured via the dial-backup PPP interface configuration commands. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname “Remote3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.1.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
```



```
 coding b8zs
 framing esf
 clock source line
 tdm-group 1 timeslots 1-24
 no shutdown
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.16 point-to-point
 frame-relay interface-dlci 16
 ip address 10.1.1.2 255.255.255.252
 dial-backup call-mode originate
 dial-backup number 5551111 analog ppp1
 dial-backup number 5552222 analog ppp1
no shutdown
!
interface ppp 1
 ip address 172.22.56.1 255.255.255.252
 ppp authentication chap
 username remoter outer password remotepass
 ppp chap hostname localrouter
 ppp chap password adtran
 no shutdown
!
ip route 192.168.2.0 255.255.255.0 172.22.56.2 255.255.255.252
!
line telnet 0 4
 password password
```

Sample configuration for central router (dialing in)

```
hostname “Central3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.100.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
 coding b8zs
 framing esf
 clock source line
```



```
 tdm-group 1 timeslots 1-24
 no shutdown
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.100 point-to-point
 frame-relay interface-dlci 100
 ip address 10.1.1.1 255.255.255.252
 dial-backup call-mode answer
 dial-backup number 555-8888 analog ppp 1
!
interface ppp 1
 ip address 172.22.56.2 255.255.255.252
 ppp authentication chap
 username localrouter password adtran
 ppp chap hostname remoterouter
 ppp chap password remotepass
 no shutdown
!
ip route 192.168.1.0 255.255.255.0 172.22.56.1 255.255.255.252

line telnet 0 4
 password password
```

Usage Examples

The following example configures AOS to generate backup calls for this endpoint using an analog modem interface (to phone number 555 1111), but never answer calls and specifies **ppp 2** as the backup interface:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup call-mode originate
(config-ppp 1)#dial-backup number 555 1111 analog ppp 2
```


Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial backup, where in the configuration AOS accesses specific routing information, etc.):

Dialing Out

1. AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number <number> on page 3077*).
3. When placing the call, AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, AOS places a call to the second number (if a second number is configured). The second number to be dialed references a separate PPP interface.

Dialing In

1. AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from caller ID, the call is terminated.

dial-backup connect-timeout <*value*>

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3070*.

Syntax Description

<*value*>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call. Valid range is **10** to **300** seconds.

Default Values

By default, the **dial-backup connect-timeout** period is set to **60** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **120** seconds before retrying a failed dial-backup call:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup connect-timeout 120**

dial-backup force

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*. Variations of this command include:

dial-backup force backup
dial-backup force primary

Syntax Description

backup	Forces backup regardless of primary link state.
primary	Forces primary link regardless of its state.

Default Values

By default, this feature is disabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to force this interface into dial backup:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup force backup**

dial-backup maximum-retry <*value*>

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*.

Syntax Description

<*value*>	Selects the number of call retries that will be made after a link failure. Valid range is **0** to **15** attempts. Setting this value to **0** will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to **0** attempts.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to retry a dial-backup call four times before considering backup operation not available:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup maximum-retry 4**

dial-backup number <*number*>

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*. Variations of this command include:

dial-backup number <*number*> **analog ppp** <*interface*>
dial-backup number <*number*> **digital-56k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>
dial-backup number <*number*> **digital-64k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>

Syntax Description

<*number*>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates the number connects to an analog modem.
digital-56k	Indicates the number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates the number belongs to a digital 64 kbps per DS0 connection.
<*isdn min chan*>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
<*isdn max chan*>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection. Range is **1** to **24** DS0s.
ppp <*interface*>	Specifies the Point-to-Point Protocol (PPP) interface to use as the backup for this interface (for example, **ppp 1**).

Default Values

By default, there are no configured dial-backup numbers.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.
Release 17.2	Command was expanded to include the cellular connections.
Release 17.3	Cellular connections were removed from this command.

Usage Examples

The following example configures AOS to dial **704-555-1212** (digital 64 kbps connection) to initiate dial-backup operation for this endpoint using interface **ppp 3** backup interface:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup number 7045551212 digital-64k 1 1 ppp 3**

dial-backup priority <*value*>

Use the **dial-backup priority** command to select the backup priority for this interface. This allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*.

Syntax Description

<*value*>	Sets the relative priority of this link. Valid range is **0** to **100**. A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to **50**.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example assigns the highest priority to this endpoint:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup priority 100**

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*.

Syntax Description

No subcommands.

Default Values

By default, AOS does not randomize the dial-backup call timers.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to randomize the dial-backup timers associated with this endpoint:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup randomize-timers**

dial-backup redial-delay <*value*>

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*.

Syntax Description

<*value*>	Specifies the delay in seconds between attempting to redial a failed backup attempt. Range is **10** to **3600** seconds.

Default Values

By default, **dial-backup redial-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures a redial delay of **25** seconds on this endpoint:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup redial-delay 25**

dial-backup restore-delay *<value>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is bouncing in and out of alarm. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*.

Syntax Description

<value>	Specifies the number of seconds AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range is **10** to **86400** seconds.

Default Values

By default, **dial-backup restore-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **30** seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup restore-delay 30**

dial-backup schedule

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial backup (as specified). For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3070*. Variations of this command include:

dial-backup schedule day <*name*>
dial-backup schedule disable-time <*value*>
dial-backup schedule enable-time <*value*>

Syntax Description

day <*name*>	Sets the days to allow backup. Valid range is Monday through Sunday.
disable-time <*value*>	Sets the time of day to disable backup. Time is entered in a 24-hour format (00:00).
enable-time <*value*>	Sets the time of day to enable backup. Time is entered in a 24-hour format (00:00).

Default Values

By default, dial backup is enabled for all days and times if the **dial-backup auto-backup** command has been issued and the dial-backup schedule has not been entered.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example enables dial backup Monday through Friday 8:00 a.m. to 7:00 p.m.:

(config)**#interface ppp 1**
(config-ppp 1)**#dial-backup schedule enable-time 08:00**
(config-ppp 1)**#dial-backup schedule disable-time 19:00**
(config-ppp 1)**#no dial-backup schedule day Saturday**
(config-ppp 1)**#no dial-backup schedule day Sunday**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface ppp 1**
(config-ppp 1)**#dynamic-dns dyndns-custom host user pass**

fair-queue

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable first in, first out (FIFO) queueing for an interface. Variations of this command include:

fair-queue
fair-queue <*threshold*>

WFQ must be enabled on an interface to use priority queuing. By default, WFQ is enabled for all interfaces with maximum bandwidth speeds equivalent to T1/E1 and below.

Syntax Description

<*threshold*>	Optional. Specifies the maximum number of packets that can be present in each conversation subqueue. Packets received for a conversation after this limit is reached are discarded. Range is **16** to **512** packets.

Default Values

By default, **fair-queue** is enabled with a threshold of **64** packets.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables WFQ on the interface with a threshold set at **100** packets:

(config)**#interface ppp 1**
(config-ppp 1)**#fair-queue 100**

hold-queue <*value*> out

Use the **hold-queue out** command to change the overall size of an interface's wide area network (WAN) output queue. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the total number of packets the output queue can contain before packets are dropped. Range is **16** to **1000** packets.

Default Values

The default queue size for weighted fair queuing (WFQ) is **400**. The default queue size for Point-to-Point Protocol (PPP) first in, first out (FIFO) and Frame Relay round-robin is **200**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the overall output queue size to **700**:

(config)**#interface ppp 1**
(config-ppp 1)**#hold-queue 700 out**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for IPv4 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Applies the named IPv4 ACL to the interface.
in	Enables access control on IPv4 packets received on the specified interface.
out	Enables access control on IPv4 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example configures the router to only allow IPv4 Telnet traffic (as defined in the user-configured **TelnetOnly** ACL) into the PPP interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface ppp 1**
(config-ppp 1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip access-policy PRIVATE**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii *<string>* **| hex** *<value>***] [client-id [***<interface>* **|** *<identifier>***]] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp client-id [*<interface>* **|** *<identifier>***] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp hostname *"<string>"* **[no-default-route | no-domain-name | no-nameservers] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track *<name>***] [***<administrative distance>***]**
ip address dhcp track *<name>* **[***<administrative distance>***]**

Syntax Description

<administrative distance>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii *<string>*	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex *<value>*	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<interface>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<identifier>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the *<identifier>* option.
hostname *<"string">*	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

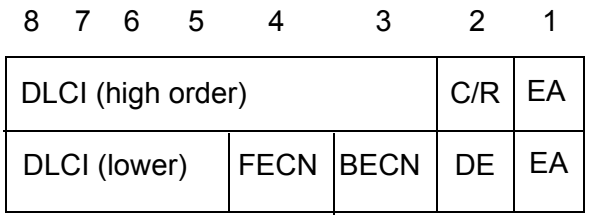
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *"<string>"* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip address dhcp hostname "adtran" no-default-route no-domain-name no-nameservers 5**

ip address negotiated

Use the **ip address negotiated** command to allow the interface to negotiate (i.e., be assigned) an IP address from the far-end Point-to-Point Protocol (PPP) connection. Use the **no** form of this command to disable the negotiation for an IP address. Variations of this command include:

ip address negotiated
ip address negotiated <*administrative distance*>
ip address negotiated <*ip address*>
ip address negotiated <*ip address*> **no-default**
ip address negotiated track <*name*>
ip address negotiated track <*name*> <*administrative distance*>

Syntax Description

<*administrative distance*>	Optional. Specifies the administrative distance to use when adding the PPP route to the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
<*ip address*>	Optional. Specifies a valid IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
no-default	Optional. Prevents the insertion of a default route. Some systems already have a default route configured and need a static route to the PPP interface to function correctly.
track <*name*>	Optional. Attaches a network monitoring track to the PPP interface. The negotiated default route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

By default, the interface is not assigned an address.

Also by default, the administrative distance value is **1**.

Command History

Release 5.1	Command was introduced.
Release 13.1	Command was expanded to include the track and administrative distance.

Usage Examples

The following example enables the PPP interface to negotiate an IP address from the far-end connection:

(config)**#interface ppp 1**
(config-ppp 1)**#ip address negotiated**

The following example enables the PPP interface to negotiate an IP address from the far-end connection without inserting a default route:

(config)**#interface ppp 1**
(config-ppp 1)**#ip address negotiated no-default**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface (only one primary address is allowed). Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 /30**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip address 192.22.72.101 /30 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

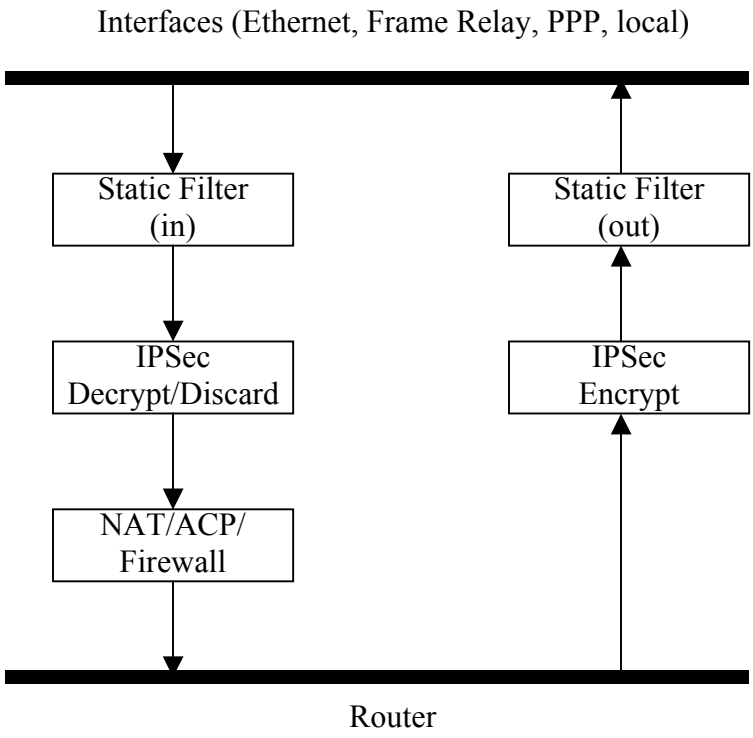
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip crypto map MyMap**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**)..

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **ppp 1**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 4 (IPv4) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries to be cleared from this IPv4 interface.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.4.0	Maximum number of stored entries was expanded to **500000** and RapidRoute is now enabled by default.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv4 interface:

(config)**#interface ppp 1**
(config-ppp 1)**#no ip ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on a Point-to-Point Protocol (**PPP)** interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248 /30 subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface ppp 1**
(config-ppp 1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 3111* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip mcast-stub downstream
```


ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*address*> command (refer to *ip igmp on page 3106*) to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include the Point-to-Point Protocol (PPP) interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 3108*, and *ip mcast-stub upstream on page 3111* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface ppp 1**
(config-ppp 1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an Internet Group Management Protocol (IGMP) proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 3108* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the Point-to-Point Protocol (PPP) interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface ppp 1**
(config-ppp 1)**#ip ospf 1 network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the Point-to-Point Protocol (PPP) 1 interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the Point-to-Point Protocol (PPP) 1 interface every **3600** seconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to **300** seconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation delay to **300** milliseconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the virtual Point-to-Point Protocol (PPP) interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP **version 1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual Point-to-Point Protocol (PPP) interface to accept only RIP **version 2** packets:

(config)**#interface ppp 1**
(config-ppp 1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP **version 1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip send version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual Point-to-Point Protocol (PPP) interface to transmit only RIP **version 2** packets:

(config)**#interface ppp 1**
(config-ppp 1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface ppp 1**
(config-ppp 1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable Internet Protocol version 4 (IPv4) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Fast switching allows an IPv4 interface to provide optimum performance when processing IPv4 traffic.

Usage Examples

The following example enables IPv4 fast switching on the PPP interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ip route-cache**

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Point-to-Point Protocol (PPP) Interface Configuration mode configures the PPP interface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface. Static routes may either use the interface name (ppp 1) or the far-end address (if it will be discovered).

Usage Examples

The following example configures the PPP interface (labeled **ppp 1**) to use the IP address assigned to the Ethernet interface (**eth 0/1**):

(config)**#interface ppp 1**
(config-ppp 1)**#ip unnumbered eth 0/1**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the Point-to-Point Protocol (PPP) interface (labeled **ppp 1**) and matches the URL filter named **MyFilter**:

(config)**#interface ppp 1**
(config-ppp 1)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on an interface. Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the interface.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the interface to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the interface.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an interface when other unicast IPv6 addresses are not needed on the interface. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the interface.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6**

ipv6 access-group *<ipv6 acl name>*

Use the **ipv6 access-group** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to be used for IPv6 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ipv6 access-group <*ipv6 acl name*> **in**
ipv6 access-group <*ipv6 acl name*> **out**

Syntax Description

<ipv6 acl name>	Applies the named IPv6 ACL to the interface.
in	Enables access control on IPv6 packets received on the specified interface.
out	Enables access control on IPv6 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 18.1	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Only one IPv6 ACL can be applied in each traffic direction.

Unlike in IPv4, IPv6 traffic filters include an implicit **permit** for neighbor solicitation and advertisement packets in an ACL before the traditional implicit **deny** at the end of the ACL. This prevents blocking of address resolution and unreachability detection, although this can be overridden by entering explicit **deny** commands in the IPv6 ACL.

Usage Examples

The following example applies the IPv6 ACL **Privatev6** to incoming IPv6 traffic on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 access-group Privatev6 in**

ipv6 access-policy *<ipv6 acp name>*

Use the **ipv6 access-policy** command to assign a specified Internet Protocol version 6 (IPv6) access control policy (ACP) to an interface. IPv6 ACPs are applied to IPv6 traffic entering an interface. Use the **no** form of this command to remove an ACP association.

Syntax Description

<ipv6 acp name>	Identifies the configured IPv6 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv6 ACPs associated with an interface.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example applies the IPv6 ACP **PRIVATEv6** to the interface:

Enable the AOS security features:
(config)**#ipv6 firewall**

Associate the ACP with the PPP interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 access-policy PRIVATEv6**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3137*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3137*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the interface and enables IPv6 processing on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address <*ipv6 link-local address*> link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<*ipv6 link-local address*>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the interface.

Default Values

By default, no IPv6 address is configured for the interface and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

A single link-local address can be manually configured on an interface. The lower 64 bits of the specified address become the Interface ID for the interface, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the interface and can be derived from the interface's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the interface.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example manually creates a link-local IPv6 address on the interface and enables IPv6 processing:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 address autoconfig

Use the **ipv6 address autoconfig** command to enable Internet Protocol version 6 (IPv6) processing on the interface, create a local-link IPv6 address for the interface, and allow the interface to automatically configure itself based on advertisements from other routers on the link. Use the **no** form of this command to remove all autoconfigured addresses, prefixes, and any resulting routes from the interface and also causes the interface to cease processing received router advertisements (RAs).Variations of this command include:

ipv6 address autoconfig
ipv6 address autoconfig default
ipv6 address autoconfig default metric <*value*>

Syntax Description

default	Optional. Specifies that the interface maintain a list of advertising routers that are willing to be IPv6 default routers.
metric <*value*>	Optional. Specifies the administrative distance for a default router maintained in the default router list. Range is **1** to **255**. Routes with lower administrative distance are favored.

Default Values

By default, no IPv6 addresses are configured for the interface and IPv6 processing is not enabled. When an IPv6 address is configured automatically, the administrative distance for default routers is **2** by default.

Command History

Release 18.1	Command was introduced.

Functional Notes

When autoconfiguration is enabled, the interface listens for RA messages that tell the interface how it should be configured. The interface then creates addresses for advertised 64-bit prefixes with the A flag in the IPv6 address set using stateless address autoconfiguration (SLAAC). The addresses use the EUI-64 interface ID in the lower 64 bits of the address. A route type of *Connected* is added to the route table if the L flag on the prefix advertisement (on-link flag) is also set.

Usage Examples

The following example enables IPv6 processing on the interface, creates a link-local IPv6 address for the interface, and allows the interface to automatically configure itself for IPv6:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address autoconfig**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname <*partial fqdn*>
ipv6 address dhcp hostname fqdn <*fqdn*>
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 3132*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address 2001:DB8:1::1/64**
(config-ppp 1)**#ipv6 address dhcp fqdn client@company.com**

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*

Use the **ipv6 address named-prefix** command to create an Internet Protocol version 6 (IPv6) address for the interface using the values in a named prefix. Use the **no** form of this command to remove the address from the interface. Variations of this command include:

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*
ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>* **eui-64**

Syntax Description

<prefix name>	Specifies the named prefix to use to create the address.
<ipv6 address/prefix-length>	Specifies the address portion appended to the named prefix to create a 128-bit host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
eui-64	Optional. Indicates that the interface ID is to be placed in the lower 64 bits of the address.

Default Values

By default, no IPv6 addresses are specified on the interface.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example creates an IPv6 address on the interface using the named prefix **PREFIX1**:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address named-prefix PREFIX1 2001:1:0:/48**

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address 2001:DB8:1::1/64**
(config-ppp 1)**#ipv6 address dhcp fqdn client@company.com**

ipv6 crypto map *<name>*

Use the **ipv6 crypto map** command to associate Internet Protocol version 6 (IPv6) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

Syntax Description

<name>	Specifies the IPv6 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Only one IPv6 crypto map can be specified per interface, and the crypto map is applied within the virtual routing and forwarding (VRF) instance to which the interface belongs. To apply the IPv6 crypto map, the interface must have IPv6 enabled. In addition, the interface must have an IPv6 address of appropriate scope to allow connectivity to peer's addresses as specified in the crypto map's entries.

Usage Examples

The following example applies all IPv6 crypto maps with the name **MyMap** to the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6**
(config-ppp 1)**#ipv6 crypto map MyMap**

ipv6 dhcp client information refresh minimum <*seconds*>

Use the **ipv6 dhcp client information refresh minimum** command to specify the minimum value the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the interface accepts as its information refresh timer. Use the **no** version of this command to return to the default setting.

Syntax Description

<*seconds*>	Specifies the refresh timer in seconds. Valid range is **600** to **3600** seconds.

Default Values

By default, the DHCPv6 client refresh timer is set to **600** seconds.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example specifies the DHCPv6 client refresh timer for the interface is **800** seconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 dhcp client information refresh minimum 800**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 dhcp client pd PREFIX1**

ipv6 dhcp relay destination <*ipv6 address*>

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination <*ipv6 address*>
ipv6 dhcp relay destination <*ipv6 address*> <*interface*>
ipv6 dhcp relay destination <*ipv6 address*> **mef-ethernet** <*slot/port*>
ipv6 dhcp relay destination <*ipv6 address*> **system-control-evc**
ipv6 dhcp relay destination <*ipv6 address*> **system-management-evc**

Syntax Description

<*ipv6 address*>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*interface*>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** <*ipv6 address*> **?** to display a list of valid interfaces.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC) is used when sending messages to the DHCPv6 server.
system-management-evc	Optional. Specifies the system management EVC is used when sending messages to the DHCPv6 server.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command *ipv6 on page 3132*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6**
(config-ppp 1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped mulitcast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the interface and specify that the interface is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the interface, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the interface. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this interface. All DHCPV^ requests received on this interface are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Enabling the interface as a DHCPv6 server using this command places the interface into DHCPv6 server mode. DHCPv6 modes (server or relay) are mutually exclusive at the interface. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the interface as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 address 2001:DB8:1::1/64**
(config-ppp 1)**#ipv6 dhcp server POOL1**

ipv6 ffe

Use the **ipv6 ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 6 (IPv6) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 ffe
ipv6 ffe max-entries <*value*>

> NOTE *Issuing this command will cause all RapidRoute entries to be cleared from this IPv6 interface.*

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled on IPv6-enabled interfaces (using the command *ipv6 on page 2231*). The default number of **max-entries** is **4096**.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv6 interface:

(config)**#interface ppp 1**
(config-ppp 1)**#no ipv6 ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the interface in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the interface.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the interface in host mode:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 mode host unicast**

ipv6 mtu *<size>*

Use the **ipv6 mtu** command to specify the maximum transmission unit (MTU) for Internet Protocol version 6 (IPv6) packets on the interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Specifies the MTU value. Valid range is **1280** to **1500** bytes.

Default Values

By default, the MTU of the interface is set to **1280** bytes.

Command History

Release 18.1	Command was introduced.

Functional Notes

In IPv6, the minimum MTU is 1280 octets. Any link that has an MTU less than 1280 octets must use link fragmentation and reassembly that is transparent to IPv6 (for example, the Fragmentation Header). Sources in the IPv6 network are expected to perform path maximum transmission unit (PMTU) discovery to send packets larger than 1280 octets. PMTU works in the following manner: First, the sending node assumes the link MTU of the interface from which the traffic is being forwarded and then sends the IPv6 packet at the link MTU size. If a router on the path is unable to forward the packet, it sends an ICMP *Packet Too Big* message back to the sending node containing the link MTU of the link on which the packet forwarding failed. The sending node then rests the PMTU to the value of the MTU field in the Internet Control Message Protocol version 6 (ICMPv6) *Packet Too Big* message, and the packet is resent.

The MTU for IPv6 packets can be set on a per-interface basis. There are two methods for setting MTUs for interfaces if required: one for Layer 3 interfaces, and one for the underlying Layer 1 and Layer 2 interfaces. For all interface types, use the **ipv6 mtu** *<size>* command to specify the IPv6 MTU in bytes from the interface's configuration mode. The minimum MTU setting for IPv6 is **1280** bytes, and the maximum is **1500** bytes. The IPv6 MTU value is independent of the IPv4 MTU setting (set with the command *ip mtu <size> on page 3112*).

When the interface is forwarding the IPv6 packet as a router, if the packet size exceeds the IPv6 MTU of the egress interface, the packet is dropped and ICMPv6 *Packet Too Big* message is sent to the source. When originating an IPv6 packet from the local IPv6 stack, and the packet is larger than the IPv6 MTU of the egress interface, the packet is fragmented and sent.

Usage Examples

The following example specifies the IPv6 MTU value for the interface:

```
(config)#interface ppp 1
(config-ppp 1)#ipv6 mtu 1350
```


ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** command to specify that the Advertisement Interval Option is sent in Internet Protocol version 6 (IPv6) router advertisement (RA) messages from the router. This command is effectual only when the interface is in router mode. Use the **no** form of this command to return to the default interval.

Syntax Description

No subcommands.

Default Values

By default, Advertisement Interval Options are not sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

Sending the Advertisement Interval Option should be enabled when the router is functioning in a mobile IP environment to aid movement detection by mobile nodes. This option contains the current value of the maximum router advertisement interval configured using the command *ipv6 nd ra interval on page 3162*.

Usage Examples

The following example specifies that the interface include Advertisement Interval Options in RA messages sent from the router:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd advertisement-interval**

ipv6 nd dad attempts *<number>*

Use the **ipv6 nd dad attempts** command to specify the number of neighbor solicitation (NS) messages sent by the interface when performing Internet Protocol version 6 (IPv6) duplicate address detection (DAD). This command is effectual when the interface is in either host or router mode. Use the **no** form of this command to return to the default value.

Syntax Description

<number>	Specifies the number of NS messages that will be sent. Range is **0** to **10** messages. A value of **0** disables DAD on the interface.

Default Values

By default, the interface sends **1** NS message.

Command History

Release 18.1	Command was introduced.

Functional Notes

DAD is used by devices to determine if IPv6 addresses are unique before they are applied to interfaces. DAD is used in NS messages to detect duplicate unicast addresses. The Target Address fields in the NS messages are set to the IPv6 address for which duplication is being detected. Destination IPv6 addresses for DAD in NS messages are the solicited-node multicast version of the address being tested. Source IPv6 addresses for DAD are set to the IPv6 unspecified address (::). Once the IPv6 address is determined by DAD to be unique, it can be applied to the IPv6 interface on the node.

DAD in AOS is performed when an interface transitions state from DOWN to UP or when manually configuring an address. When performing DAD because of an interface transition, DAD will happen immediately after the interface transition and again 40 seconds later to cooperate with the port being connected to an Ethernet switch.

Usage Examples

The following example specifies that **3** NS messages are sent by the interface when performing DAD:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd dad attempts 3**

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command to specify the M flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. The M flag instructs hosts receiving the RA that they can use stateful Dynamic Host Configuration Protocol version 6 (DHCPv6) to configure addresses and nonaddress information. Use the **no** form of this command to disable the setting of the M flag.

Syntax Description

No subcommands.

Default Values

By default, the M flag is not set in RAs.

Command History

Release 18.1	Command was introduced.

Functional Notes

If you specify that the M flag is set in RA messages, you do not need to set the 0 flag (it becomes redundant).

Usage Examples

The following example sets the M flag for RA messages sent by the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd managed-config-flag**

ipv6 nd ns-interval *<value>*

Use the **ipv6 nd ns-interval** command to specify the interval between transmission of certain Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages and to control what ND value is advertised in router advertisement (RA) messages. This command is effectual whether the interface is in host or router mode. Use the **no** form of this command to return the interval to the default value.

Syntax Description

<value>	Specifies the time (in milliseconds) between neighbor message transmissions. Valid range is **1000** to **3600000** ms.

Default Values

By default, the interval is set to **1000** ms for internal use by the router and **0** (unspecified) is sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command controls the spacing of neighbor solicitation (NS) messages for functions such as address resolution, reachability detection, and duplicate address detection (DAD). For DAD it also serves as the amount of time after the last transmission before the detection phase of autoconfiguration terminates. In addition, the command controls the interval between unsolicited neighbor advertisement (NA) messages.

Usage Examples

The following example changes the interval between RA messages sent from the interface to **2000** ms:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd ns-interval 2000**

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command to specify the O flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. When the O flag is set, hosts receiving the RA messages are instructed that they may use stateless Dynamic Host Configuration Protocol version 6 (DHCPv6) to receive information that is not IPv6 addressing information, and to use some other method (whether through manual configuration, stateless address autoconfiguration (SLAAC), etc.) for addressing information. Use the **no** form of this command to disable the O flag setting.

Syntax Description

No subcommands.

Default Values

By default, the O flag is not set in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

If the M flag is set for RA messages, you do not need to set the O flag.

Usage Examples

The following example sets the O flag in RA messages from the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd other-config-flag**

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the interface. Use the **no** form of this command to remove the specified prefix configuration from the interface. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the interface is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the interface. Prefixes for IPv6 addresses configured on a router interface are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the interface.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ipv6 nd purge-timer <*value*>

Use the **ipv6 nd purge-timer** command to specify the maximum amount of time an unused Internet Protocol version 6 (IPv6) neighbor entry remains in the neighbor cache. This command applies to interfaces in either host or router mode. Use the **no** form of this command to return the purging interval to the default value.

Syntax Description

<*value*>	Specifies the neighbor cache entry storage time in minutes. Valid range is **10** to **1440** minutes.

Default Values

By default, idle (STALE) neighbor cache entries are cleared after **1440** minutes (24 hours).

Command History

Release 18.1	Command was introduced.

Functional Notes

This command applies to interfaces in either router or host mode. A neighbor entry is typically purged when neighbor unreachability detection (NUD) is invoked and the neighbor is determined to no longer be reachable. However, NUD is not performed on idle (STALE) neighbor entries, so this command provides a method for purging unused entries after a specified amount of time.

Usage Examples

The following example specifies that idle neighbor entries in the neighbor cache are removed after **800** minutes:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd purge-timer 800**

ipv6 nd ra interval

Use the **ipv6 nd ra interval** command to specify the interval between transmission of Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 nd ra interval *<max time>*
ipv6 nd ra interval *<max time> <min time>*
ipv6 nd ra interval msec *<max time>*
ipv6 nd ra interval msec *<max time> <min time>*

Syntax Description

<max time>	Specifies the maximum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **4** to **1800** seconds and **70** to **1800000** ms.
<min time>	Optional. Specifies the minimum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **3** seconds to 75 percent of the configured maximum time value in seconds, or **30** ms to 75 percent of the configured maximum time value in ms.
msec	Optional. Specifies that the time values are in milliseconds.

Default Values

By default, the interval is set in seconds and has a maximum interval time of **200** seconds and a minimum interval time of 75 percent of the maximum seconds value, but not less than **3** seconds.

Command History

Release 18.1	Command was introduced.

Functional Notes

If this router is used as a default router, the interval between RA messages should not be set to a larger value than the RA lifetime set by the command *ipv6 nd ra lifetime <value> on page 3163*, which has a default value of **1800** seconds.

Usage Examples

The following example specifies that the maximum interval in seconds between RA message transmissions is **300**:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd ra interval 300**

ipv6 nd ra lifetime <*value*>

Use the **ipv6 nd ra lifetime** command to specify the router lifetime advertised in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is effectual when the interface is in router mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

ipv6 nd ra lifetime <*value*>
ipv6 nd ra lifetime default-route

Syntax Description

<*value*>	Specifies the router lifetime in seconds. Range is **0** to **9000** seconds. A value of **0** indicates this is not a default router. A value other than 0 indicates to other nodes that this router can be used as a default router.
default-route	Specifies the RA lifetime is **0** if no default route exists on any IPv6 interface.

Default Values

By default, the router lifetime is set to **1800** seconds.

Command History

Release 18.1	Command was introduced.
Release R11.5.0	Command was expanded to include the **default-route** parameter.

Functional Notes

A value other than **0** for a router lifetime should be larger than the router advertisement interval specified in the command *ipv6 nd ra interval on page 3162*.

Usage Examples

In the following example, the router lifetime advertised in RA messages is **3000** seconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd ra lifetime 3000**

ipv6 nd ra reachable-time <*value*>

Use the **ipv6 nd ra reachable-time** command to specify the value advertised for reachable time in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command also specifies the internal base reachable time used by the router. This command is effectual for interfaces in either host or router mode. Use the **no** form of this command to return the reachability value to the default setting.

Syntax Description

<*value*>	Specifies the reachability time in milliseconds. Range is **0** to **3600000** ms. A value of **0** indicates the reachable time is unspecified.

Default Values

By default, the router advertises a reachability time of **0** ms and uses an internal value of **30000** ms.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command is effectual for interfaces in either router or host mode. For hosts, this value sets the internal reachable time used by the host if no RAs are received specifying a different value. For routers, the value indicates the amount of time a device is considered reachable after having received a reachability confirmation in neighbor unreachabililty detection (NUD).

Usage Examples

The following example specifies that a reachability time of **50000** ms is advertised in RA messages:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd ra reachable-time 50000**

ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command to specify whether Internet Protocol version 6 (IPv6) router advertisement (RA) messages will be suppressed. This command only applies to interfaces in router mode. Use the **no** form of this command to begin sending RA messages.

Syntax Description

No subcommands.

Default Values

By default, RA messages are not suppressed. When IPv6 routing is not enabled on the router, or when implemented in a host-only mode, the default setting is to suppress advertisements on all interface types.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example suppresses RA messages on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd ra suppress**

ipv6 nd router-preference

Use the **ipv6 nd router-preference** command to specify the default router preference value set in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. Setting this preference helps the receivers of RA messages to determine the preference of one router over another as a default router in environments with multiple routers. Use the **no** form of this command to return the preference to the default setting. Variations of this command include:

ipv6 nd router-preference high
ipv6 nd router-preference low
ipv6 nd router-preference medium

Syntax Description

high	Specifies the preference value is high.
low	Specifies the preference value is low.
medium	Specifies the preference value is medium.

Default Values

By default, the router preference is set to medium.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that the advertised default router preference is high:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 nd router-preference high**

ipv6 route-cache

Use the **ipv6 route-cache** command to enable Internet Protocol version 6 (IPv6) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 18.2	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Fast switching allows an IPv6 interface to provide optimum performance when processing IPv6 traffic.

Usage Examples

The following example enables IPv6 fast switching on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ipv6 route-cache**

keepalive *<value>*

Use the **keepalive** command to enable the transmission of keepalive packets on the interface and specify the time interval in seconds between transmitted packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Defines the time interval (in seconds) between transmitted keepalive packets. Valid range is **0** to **32767** seconds.

Default Values

By default, the time interval between transmitted keepalive packets is **10** seconds.

Command History

Release 1.1	Command was introduced.

Functional Notes

If three keepalive packets are sent to an interface with no response, the interface is considered down. To detect interface failures quickly, specify a smaller keepalive time.

Usage Examples

The following example specifies a keepalive time of **5** seconds on the virtual Point-to-Point Protocol (PPP) interface:

(config)**#interface ppp 1**
(config-ppp 1)**#keepalive 5**

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the Point-to-Point Protocol (PPP) interface to receive LLDP packets:

(config)**#interface ppp 1**
(config-ppp 1)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to disable this feature. Variations of this command include:

lldp send management-address
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

By default, all interfaces are configured to transmit and receive LLDP packets of all types.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the Point-to-Point Protocol (PPP) interface to transmit LLDP packets containing all enabled information types:

(config)**#interface ppp 1**
(config-ppp 1)**#lldp send**

The following example configures the PPP interface to transmit and receive LLDP packets containing all information types:

(config)**#interface ppp 1**
(config-ppp 1)**#lldp send-and-receive**

max-reserved-bandwidth <*value*>

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<*value*>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range: **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies **85** percent of the bandwidth on the Point-to-Point Protocol (PPP) 1 be available for use in user-defined queues:

(config)**#interface ppp 1**
(config-ppp 1)**#max-reserved-bandwidth 85**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip primary vrrp <*number*>
media-gateway ip primary vrrpv3 <*number*>
media-gateway ip secondary <*ipv4 address*>
media-gateway ip secondary vrrp <*number*>
media-gateway ip secondary vrrp <*number*> <*ipv4 address*>
media-gateway ip secondary vrrpv3 <*number*>
media-gateway ip secondary vrrpv3 <*number*> <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrrp <*number*>	Specifies that the IPv4 address of the Virtual Router Redundancy Protocol version 2 (VRRP) router group's virtual router ID (VRID) is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
vrrpv3 <*number*>	Specifies that the IPv4 address of the VRRP version 3 (VRRPv3) VRID is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
<*ipv4 address*>	Optional. Specifies a secondary IPv4 address of the VRRP or VRRPv3 VRID is used as the media gateway address on the interface. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A4.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.
Release R12.2.0	Command was expanded to include the **vrrp** and **vrrpv3** parameters.

Functional Notes

To use VRRP or VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRP or VRRPv3.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface ppp 1**
(config-ppp 1)**#media-gateway ip primary**

media-gateway ipv6

Use the **media-gateway ipv6** command to associate an Internet Protocol version 6 (IPv6) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv6 address associated with it. However, some interfaces allow dynamic configuration of IPv6 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ipv6
media-gateway ipv6 <*ipv6 address*>
media-gateway ipv6 loopback <*interface id*>
media-gateway ipv6 vrrpv3 <*number*>
media-gateway ipv6 vrrpv3 <*number*> <*ipv6 address*>

Syntax Description

<*ipv6 address*>	Specifies an IPv6 address to use for the media gateway. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
loopback <*interface id*>	Specifies an IPv6 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv6 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
vrrpv3 <*number*>	Specifies that all the secondary IPv6 addresses of the Virtual Routing Redundancy Protocol version 3 (VRRPv3) virtual router ID (VRID) are used as media gateway addresses on the interface. Valid VRID range is **1** to **255**.
<*ipv6 address*>	Optional. Specifies a single IPv6 address of the VRRPv3 VRID is used as the media gateway address on the interface. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

Default Values

By default, **media-gateway ipv6** is disabled.

Command History

Release R10.8.0	Command was introduced.
Release R12.2.0	Command was expanded to include the **vrrpv3** parameters.

Functional Notes

To use VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRPv3.

Usage Examples

The following example configures the unit to use the IPv6 address for RTP traffic:

(config)**#interface ppp 1**
(config-ppp 1)**#media-gateway ipv6**

ospfv3 <*process id*> **area** <*area id*>

Use the **ospfv3 area** command to add an interface to an Open Shortest Path First version 3 (OSPFv3) process, and to configure the OSPFv3 process on the interface. This command places the interface in the specified area for the specified Internet Protocol version 6 (IPv6) OSPFv3 address family, and optionally defines the instance ID that is used to represent this OSPFv3 process in messages on the interface's link. Use the **no** form of this command to remove the OSPFv3 process from the interface. Variations of this command include:

ospfv3 <*process id*> **area** <*area id*> **ipv6**
ospfv3 <*process id*> **area** <*area id*> **ipv6 instance** <*instance id*>

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join, for the specified address family. The process ID is locally significant to the device, and must be unique among all OSPFv3 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the given OSPFv3 process. Valid range is **0** to **4294967295**.
ipv6	Identifies the OSPFv3 address family as IPv6.
instance <*instance id*>	Optional. Specifies the value to use in the instance ID field of messages sent or received by this OSPFv3 process on the interface's link. Valid range is **0** to **31**.

Default Values

By default, an OSPFv3 process is not configured on an interface. By default, process IDs, area IDs, and instance IDs are not defined.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

When using this command to enable an OSPFv3 process on an interface, keep the following rules in mind:

- The interface must have the address family enabled on the interface. If the address family is not enabled on the interface, the command is rejected and an error is displayed.
- Only interfaces on the default virtual routing and forwarding (VRF) instance support this command. Interfaces on a nondefault VRF will display an error when you attempt to configure OSPFv3 settings.
- The interface and the specified OSPFv3 process (if defined in the global configuration) must be in the same VRF or the command will fail.
- The address family must match that specified for the OSPFv3 process if the process has been defined in the global configuration or the command will fail.
- If the OSPFv3 process identified by the process ID does not exist in the global configuration, it is automatically created, along with the specified address family, and it is assigned to the VRF of which the interface is a member.

- If the specified OSPFv3 process is already at its maximum limit of processes or address families, the command fails.
- If the specified OSPFv3 process already exists in the global configuration, but its configuration does not include an address family, the specified address family is added to the OSPFv3 router configuration.
- A given OSPFv3 process can only have one address family.
- Multiple OSPFv3 instances per address family, per VRF, can be created and can be assigned to a given interface.
- If the interface's VRF changes, all OSPFv3 assignments are removed.
- To change an OSPFv3 process's VRF, the process must first be removed and then recreated. Removing the process removes all OSPFv3 assignments for that process form all interfaces.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To add an interface to the OSPFv3 process **5**, in area **10**, with an instance ID of **10**, enter the command as follows:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 5 area 10 ipv6 instance 10**

ospfv3 authentication

Use the **ospfv3 authentication** command to authenticate an interface that is performing Internet Protocol version 6 (IPv6) Open Shortest Path First version 3 (OSPFv3) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ospfv3 authentication ipsec spi <*spi*> **md5** <*key*>
ospfv3 authentication ipsec spi <*spi*> **sha1** <*key*>
ospfv3 authentication null

Syntax Description

ipsec	Specifies that IP security (IPsec) authentication is used.
spi <*spi*>	Specifies the security parameter index (SPI). Valid range is **256** to **4294967295**.
md5 <*key*>	Specifies that MD5 authentication is used. Keys are specified in 32 hexadecimal characters.
sha1 <*key*>	Specifies that SHA-1 authentication is used. Keys are specified in 40 hexadecimal characters.
null	Specifies that no OSPFv3 authentication is used.

Default Values

By default, this is set to **null** (meaning no authentication is used).

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example specifies that no OSPFv3 authentication will be used on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 authentication null**

ospfv3 <*process id*> cost <*cost*>

Use the **ospfv3 cost** command to specify a value that represents the cost of sending an Open Shortest Path First version 3 (OSPFv3) packet over the interface. Use the **no** form of this command to return the cost to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
cost <*cost*>	Specifies the OSPFv3 cost of the interface. This value overrides any automatically computed cost value (default value). Valid range is **1** to **65535**.

Default Values

By default, the OSPFv3 cost of the interface is automatically computed. The automatic cost computation is the reference bandwidth divided by the interface bandwidth. The reference bandwidth is set by the command *auto-cost reference-bandwidth <value> on page 4150*, and defaults to **100** Mbps.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the OSPFv3 cost of the interface as **10**:

```
(config)#interface ppp 1
(config-ppp 1)#ospfv3 5 cost 10
```


ospfv3 <*process id*> dead-interval <*value*>

Use the **ospfv3 dead-interval** command to specify the maximum interval allowed between Open Shortest Path First version 3 (OSPFv3) Hello packets on the interface. If the maximum interval is exceeded, neighboring devices will assume that the device is down. This value must be the same across all interfaces on a link. Use the **no** form of this command to return the dead interval to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
dead-interval <*value*>	Specifies the maximum number of seconds allowed between OSPFv3 Hello packets. It is recommended that this value be **4** times the Hello packet interval (set with the command *ospfv3 <process id> hello-interval <value> on page 3184*). Valid range is **1** to **65535** seconds.

Default Values

By default, the maximum interval allowed between OSPFv3 Hello packets is set to **40** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To specify the dead interval between OSPFv3 Hello packets on the interface, enter the command as follows:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 5 dead-interval 100**

ospfv3 encryption

Use the **ospfv3 encryption** command to specify a symmetrical, bidirectional Open Shortest Path First version 3 (OSPFv3) security association (SA) that uses encapsulating security payload (ESP) for encryption and authentication of all OSPFv3 messages that are sent or received on the interface. This command allows you to specify OSPFv3 security at the interface level. Use the **no** form of this command to remove IP security (IPsec) protection of OSPFv3 messages on the interface. Variations of this command include:

ospfv3 encryption ipsec spi <*spi*> **esp** <*encryption type*> <*encryption key*> <*authentication type*> <*authentication key*>
ospfv3 encryption ipsec spi <*spi*> **esp null** <*authentication type*> <*authentication key*>
ospfv3 encryption null

Syntax Description

ipsec	Specifies that IPsec encryption is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by any other IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
esp	Specifies that ESP is used.
null	Specifies that OSPFv3 messages on this interface are not encrypted when used in the **ospfv3 encryption null** format (even when encryption is specified by the OSPFv3 area configuration). When used in the **ospfv3 encryption ipsec spi** <*spi*> **esp null** format, **null** indicates that messages on the interface will not be encrypted, but will be authenticated.
<*encryption type*>	Specifies the type of algorithm used to encrypt OSPFv3 messages. Valid values for encryption are: **3des** uses triple data encryption standard (DES). **aes-cbc** uses advanced encryption standard (AES) with cipher block chaining (CBC). Select from **aes-cbc 128**, **aes-cbc 192**, or **aes-cbc 256**. **des** uses DES.
<*encryption key*>	Specifies the hexadecimal encryption key. The size of the encryption key is determined by the respective encryption algorithm, as follows: **3des** uses a **48** character key size. **aes-cbc 128** uses a **32** character key size. **aes-cbc 192** uses a **48** character key size. **aes-cbc 256** uses a **64** character key size. **des** uses a **16** character key size.
<*authentication type*>	Specifies the algorithm used for authenticating OSPFv3 messages. Valid authentication methods are Message-Digest 5 (**md5**) and Secure-Hash 1 (**sha1**) algorithms.

<authentication key> Specifies the hexadecimal authentication key. The size of the authentication key is determined by the respective authentication algorithm, as follows:

md5 uses a **32** character key size.

sha1 uses a **40** character key size.

Default Values

By default, there is no security for OSPFv3 messages on an interface.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

This commands specifies OSPFv3 security at the interface level. Protection specified with this command overrides any area-level OSPFv3 protection that might apply to the interface.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages with an SPI of **120**, no encryption, and **md5** as the authentication method:

```
(config)#interface ppp 1
(config-ppp 1)#ospfv3 encryption ipsec spi 120 esp null md5
    NeWtStpsswdLoonGpsswDhtThmnWoKEY
```

ospfv3 <*process id*> hello-interval <*value*>

Use the **ospfv3 hello-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) Hello packets sent on the interface. This value must be the same across all interfaces on the link. Use the **no** form of this command to return the Hello packet interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
hello-interval <*value*>	Specifies the number of seconds allowed between OSPFv3 Hello packets. Valid range is **1** to **65535** seconds.

Default Values

By default, the Hello packet interval for OSPFv3 is **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the interval between OSPFv3 Hello packets on the interface is **20** seconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 5 hello-interval 20**

ospfv3 <*process id*> network

Use the **ospfv3 network** command to specify the network type for Open Shortest Path First version 3 (OSPFv3) enabled interfaces. Use the **no** form of this command to return the interface's network type to the default value. Variations of this command include:

ospfv3 <*process id*> **network broadcast**
ospfv3 <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
broadcast	Specifies that the OSPFv3 network type for the interface is set to broadcast.
point-to-point	Specifies that the OSPFv3 network type for the interface is set to point-to-point.

Default Values

By default, Ethernet interfaces are set to network type broadcast, and point-to-point (PPP), Frame Relay, and loopback interfaces are set to network type point-to-point.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the network interface as point-to-point:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 5 network point-to-point**

ospfv3 <*process id*> priority <*value*>

Use the **ospfv3 priority** command to specify the Open Shortest Path First version 3 (OSPFv3) priority for the interface. Use the **no** form of this command to return the interface's priority to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
priority <*value*>	Specifies the OSPFv3 priority for the interface. Valid range is **0** to **255**.

Default Values

By default, the OSPFv3 priority of an interface is set to **1**.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

Priority is used in the election of the designated router and backup designated router on multi-access networks. Interfaces connected to multi-access networks (such as Ethernet interfaces) perform an election for a designated and backup designated router. The router interface with the highest OSPFv3 priority on the link becomes the designated router for that link. The interface with the next highest priority becomes the designated backup router. In the event there is a tie, the router interface with the highest router ID takes precedence. A priority value of **0** indicates the router is ineligible to become either the designated or backup designated router.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's OSPFv3 priority value to **6**:

```
(config)#interface ppp 1
(config-ppp 1)#ospfv3 5 priority 6
```

ospfv3 <*process id*> retransmit-interval <*value*>

Use the **ospfv3 retransmit-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) sent on the interface. Use the **no** form of this command to return the OSPFv3 LSA interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
retransmit-interval <*value*>	Specifies the number of seconds between OSPFv3 LSAs sent on the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA retransmit interval is set to **5** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the LSA retransmit interval is **10** seconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 5 retransmit-interval 10**

ospfv3 <*process id*> shutdown

Use the **ospfv3 shutdown** command to disable an Open Shortest Path First version 3 (OSPFv3) process on the interface. When this command is used, the OSPFv3 commands remain in place, but logically it appears to the interface as though the OSPFv3 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv3 process.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables OSPFv3 process **5** on the interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 5 shutdown**

ospfv3 <*process id*> transmit-delay <*value*>

Use the **ospfv3 transmit-delay** command to specify the estimated time that is required to propagate an Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) on the interface. Use the **no** form of this command to return the transmit delay to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3177*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
transmit-delay <*value*>	Specifies the number of seconds required to send LSAs from the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA transmit delay is set to **1** second.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's LSA transmit delay to **2** seconds:

(config)**#interface ppp 1**
(config-ppp 1)**#ospfv3 5 transmit-delay 2**

peer default ip address *<ipv4 address>*

Use the **peer default ip address** command to specify the default peer Internet Protocol version 4 (IPv4) address of the remote end of this interface. Use the **no** form of this command to remove an assigned IPv4 address.

Syntax Description

<ipv4 address>	Specifies the default peer IPv4 address for the remote end. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there is no assigned default peer IPv4 address.

Command History

Release 3.1	Command was introduced.

Functional Notes

This command is useful if the peer does not send the IPv4 address option during Point-to-Point Protocol (PPP) negotiations.

Usage Examples

The following example sets the default peer IPv4 address to **192.22.71.50**:

(config)**#interface ppp 1**
(config-ppp 1)**#peer default ip address 192.22.71.50**

peer default ipv6 interface-id *<interface id>*

Use the **peer default ipv6 interface-id** command to specify the default peer Internet Protocol version 6 (IPv6) interface ID of the remote end of this interface. Use the **no** form of this command to remove an assigned IPv6 interface ID.

Syntax Description

<interface id>	Specifies the default peer IPv6 interface ID for the remote end. IPv6 interface IDs should be expressed in colon hexadecimal notation (**X:X:X:X**). For example, **2AA:FF:FE3F:2A1C**.

Default Values

By default, there is no assigned default peer IPv6 interface ID.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example sets the default peer IPv6 interface ID to **2AA:FF:FE3F:2A1C**:

(config)**#interface ppp 1**
(config-ppp 1)**#peer default ipv6 interface-id 2AA:FF:FE3F:2A1C**

ppp authentication

Use the **ppp authentication** command to specify the authentication protocol on the Point-to-Point Protocol (PPP) virtual interface that the peer should use to authenticate itself. Use the **no** form of this command to disable this feature. Variations of this command include:

ppp authentication chap
ppp authentication pap

Syntax Description

chap	Configures Challenge-Handshake Authentication Protocol (CHAP) on the interface.
pap	Configures Password Authentication Protocol (PAP) on the interface.

Default Values

By default, PPP endpoints have no authentication configured.

Command History

Release 1.1	Command was introduced.

Technology Review

CHAP and PAP are two authentication methods that enjoy widespread support. Both methods are included in AOS and are easily configured.

The authentication method set up on the local router can be different from that on the peer. Also, just because one router requires authentication from its peer does not mean it also has to authenticate itself to the peer.

Defining PAP

PAP is used to verify that the PPP peer is a permitted device by checking a user name and password configured on the peer. The user name and password are both sent unencrypted across the connecting private circuit.

PAP requires two-way message passing. First, the router that is required to be authenticated (for example, the peer) sends an authentication request with its user name and password to the router requiring authentication (for example, the local router). The local router then looks up the user name and password in the user name database within the PPP interface, and if they match sends an authentication acknowledge back to the peer.

The PPP user name and password database is separate and distinct from the global user name password database. For PAP and CHAP, use the database under the PPP interface configuration.

Several example scenarios are given below for clarity.

Configuring PAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (host name **Local**):

Local(config-ppp 1)**#ppp authentication pap**
Local(config-ppp 1)**#username farend password far**

On the peer (host name **Peer**):

Peer(config-ppp 1)**#ppp pap sent-username farend password far**

The first line of the configuration sets the authentication mode as PAP. This means the peer is required to authenticate itself to the local router via PAP. The second line is the user name and password expected to be sent from the peer. On the peer, the **ppp pap sent-username** command is used to specify the appropriate matching user name and password.

Configuring PAP Example 2: Both routers require the peer to authenticate itself.

On the local router (host name **Local**):

Local(config-ppp 1)**#ppp authentication pap**
Local(config-ppp 1)**#username farend password far**
Local(config-ppp 1)**#ppp pap sent-username nearend password near**

On the peer (host name **Peer**):

Peer(config-ppp 1)**#ppp authentication pap**
Peer(config-ppp 1)**#username nearend password near**
Peer(config-ppp 1)**#ppp pap sent-username farend password far**

Now both routers send the authentication request, verify that the user name and password sent match what is expected in the database, and send an authentication acknowledge.

Defining CHAP

CHAP is a three-way authentication protocol composed of a challenge response and success or failure. The message digest 5 (MD5) protocol is used to protect user names and passwords in the response.

First, the local router (requiring its peer to be authenticated) sends a challenge containing the unencrypted user name of the peer and a random number. The user name of the peer is found in the user name database within the PPP interface of the local router. The peer then looks up the user name in the user name database within the PPP interface, and if found takes the corresponding password and its own host name and sends a response back to the local router. This data is encrypted. The local router verifies that the user name and password are in its own user name database within the PPP interface, and if so sends a success back to the peer.

The PPP user name and password database is separate and distinct from the global user name password database. For PAP and CHAP, use the database under the PPP interface configuration.

Several example scenarios are given below for clarity.

Configuring CHAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (host name **Local**):

Local(config-ppp 1)**#ppp authentication chap**
Local(config-ppp 1)**#username Peer password same**

On the peer (host name **Peer**):

Peer(config-ppp 1)**#ppp chap password same**

The first line of this configuration sets the authentication mode to CHAP. This means the peer is required to authenticate itself to the local router via CHAP. The second line is the user name and password expected to be sent from the peer. The peer uses its **hostname** and **ppp chap password** commands to send the proper authentication information.

Both ends must have identical passwords.

Configuring CHAP Example 2: Using the ppp chap hostname command as an alternate solution.

On the local router (host name **Local**):

Local(config-ppp 1)**#ppp authentication chap**
Local(config-ppp 1)**#username farend password same**

On the peer (host name **Peer**):

Peer(config-ppp 1)**#ppp chap hostname farend**
Peer(config-ppp 1)**#ppp chap password same**

Notice the local router is expecting user name **farend** even though the peer router's host name is **Peer**. Therefore, the peer router can use the **ppp chap hostname** command to send the correct name in the challenge.

Both ends must have identical passwords.

Configuring CHAP Example 3: Both routers require each other to authenticate themselves using the same shared password.

On the local router (host name **Local**):

Local(config-ppp 1)**#ppp authentication chap**
Local(config-ppp 1)**#username Peer password same**

On the peer (host name **Peer**):

Peer(config-ppp 1)**#ppp authentication chap**
Peer(config-ppp 1)**#username Local password same**

This is basically identical to Example 1 except that both routers will now challenge each other and respond.

Both ends must have identical passwords.

Configuring CHAP Example 4: Both routers require each other to authenticate themselves using two separate shared passwords.

On the local router (host name **Local**):

Local(config-ppp 1)**#ppp authentication chap**
Local(config-ppp 1)**#username Peer password far**
Local(config-ppp 1)**#ppp chap password near**

On the peer (host name **Peer**):

Peer(config-ppp 1)**#ppp authentication chap**
Peer(config-ppp 1)**#username Local password near**
Peer(config-ppp 1)**#ppp chap password far**

This is basically identical to Example 3, except that there are two separate shared passwords.

Notice this example has both ends using different sets of passwords.

Configuring CHAP Example 5: Using the ppp chap hostname command as an alternate solution.

On the local router (host name **Local**):

Local(config-ppp 1)**#ppp authentication chap**
Local(config-ppp 1)**#username farend password far**
Local(config-ppp 1)**#ppp chap hostname nearend**
Local(config-ppp 1)**#ppp chap password near**

On the peer (host name **Peer**):

Peer(config-ppp 1)**#ppp authentication chap**
Peer(config-ppp 1)**#username nearend password near**
Peer(config-ppp 1)**#ppp chap hostname farend**
Peer(config-ppp 1)**#ppp chap password far**

Notice the local router is expecting user name **farend** even though the peer router's host name is **Peer**. Therefore, the peer router can use the **ppp chap hostname** command to send the correct name on the challenge.

Notice this example has both ends using different sets of passwords.

ppp bcp tagged-frame

Use the **ppp bcp tagged-frame** command to allow negotiation of IEEE 802.1Q-tagged packets over Bridging Control Protocol (BCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example configures Point-to-Point Protocol (PPP) interface 1 to negotiate tagged frames over BCP:

(config)**#interface ppp 1**
(config-ppp 1)**#ppp bcp tagged-frame**

ppp chap hostname *<name>*

Use the **ppp chap hostname** command to configure an alternate host name for Challenge-Handshake Authentication Protocol (CHAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured host name. For more information on Password Authentication Protocol (PAP) and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication on page 3192*.

Syntax Description

<name>	Specifies a host name using an alphanumeric string up to 80 characters in length.

Default Values

By default, there are no configured PPP CHAP host names.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a PPP CHAP host name of **my_host**:

(config)**#interface ppp 1**
(config-ppp 1)**#ppp chap hostname my_host**

ppp chap password *<password>*

Use the **ppp chap password** command to configure an alternate password when the peer requires Challenge-Handshake Authentication Protocol (CHAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured password. For more information on Password Authentication Protocol (PAP) and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication on page 3192*.

Syntax Description

<password>	Specifies a password using an alphanumeric string up to 80 characters in length.

Default Values

By default, there is no defined PPP CHAP password.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a PPP CHAP password of **my_password**:

(config)**#interface ppp 1**
(config-ppp 1)**#ppp chap password my_password**

ppp mtu *<size>*

Use the **ppp mtu** command to configure the Point-to-Point Protocol (PPP) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Configures the window size for transmitted packets. The valid range is **64** to **2100** bytes.

Default Values

By default, the PPP MTU on an interface is set to **1500** bytes.

Command History

Release 17.9	Command was introduced.

Usage Examples

The following example specifies a PPP MTU of **1200** on the PPP interface:

(config)**#interface ppp 1**
(config-ppp 1)**#ppp mtu 1200**

ppp multilink

Use the **ppp multilink** command to enable Multilink Point-to-Point Protocol (MLPPP) operation on an existing Point-to-Point Protocol (PPP) interface. Use the **no** form of this command to disable this feature. Variations of this command include:

ppp multilink fragmentation
ppp multilink interleave
ppp multilink maximum <*number*>

Syntax Description

fragmentation	Enables multilink fragmentation operation.
interleave	Enables multilink interleave operation.
maximum <*number*>	Specifies the maximum number of links allowed in a PPP multilink bundle.

Default Values

By default, MLPPP is disabled.

Command History

Release 7.1	Command was introduced.
Release 7.2	Fragmentation and interleave operation were added.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

When enabled, this interface is capable of the following:

- Combining multiple physical links into one logical link.
- Receiving upper layer protocol data units (PDUs), fragmenting and transmitting over the physical links.
- Receiving fragments over the physical links and reassembling them into PDUs.

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

The multilink bundle will remain active with a minimum of one physical link. Physical links may be dynamically added or removed from the multilink bundle with minor interruption to traffic flow.

Usage Examples

The following example enables MLPPP:

(config)**#interface ppp 1**
(config-ppp 1)**#ppp multilink**

ppp pap sent-username <*username*> password <*password*>

Use the **ppp pap sent-username password** command to configure a user name and password when the peer requires Password Authentication Protocol (PAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured password. For more information on PAP and Challenge-Handshake Authentication Protocol (CHAP) functionality, refer to the *Technology Review* section for the command *ppp authentication on page 3192*.

Syntax Description

<username>	Specifies a user name by alphanumeric string up to 80 characters in length (the user name is case sensitive).
<password>	Specifies a password by alphanumeric string up to 80 characters in length (the password is case sensitive).

Default Values

By default, there is no defined **ppp pap sent-username** and **password**.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a PPP PAP sent user name of **local** and a password of **my_password**:

(config)**#interface ppp 1**
(config-ppp 1)**#ppp pap sent-username local password my_password**

pppoe ac-name *<name>*

Use the **pppoe ac-name** command to identify the access controller (AC) with which AOS expects to establish a Point-to-Point Protocol over Ethernet (PPPoE) session. Use the **no** form of this command to return to the default setting.

Syntax Description

<name>	Specifies an AC by text string (up to 255 characters) corresponding to the AC-Name Tag under RFC 2516. If this field is not specified, any AC is acceptable. The AC value may be a combination of trademark, model, and serial ID information (or simply the medium access control (MAC) address of the unit).

Default Values

By default, no AC is specified.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example identifies the AC with which AOS expects to establish a PPPoE session:

(config)**#interface ppp 1**
(config-ppp 1)**#pppoe ac-name Access_Controller_Name**

pppoe service-name <*name*>

Use the **pppoe service-name** command to use this tag value to filter Point-to-Point Protocol over Ethernet (PPPoE) session offers from PPPoE servers. Use the **no** form of this command to return to the default setting.

Syntax Description

<*name*>	Specifies a service name by text string (up to 255 characters) corresponding to the Service-Name Tags under RFC 2516. This string indicates an Internet service provider (ISP) name (or a class of service (CoS) or quality of service (QoS)). If this field is not specified, any service is acceptable.

Default Values

By default, no names are specified.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example defines a service type that is not to be accepted by AOS:

(config)**#interface ppp 1**
(config-ppp 1)**#pppoe service-name Service_Name**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing (WFQ).
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the Point-to-Point Protocol (PPP) 1 interface:

(config)**#interface ppp 1**
(config-ppp 1)**#qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the virtual Point-to-Point Protocol (PPP) interface:

(config)**#interface ppp 1**
(config-ppp 1)**#rtp quality-monitoring**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.2	Command was expanded to the cellular interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the virtual Point-to-Point Protocol (PPP) interface:

(config)**#interface ppp 1**
(config-ppp 1)**#no snmp trap link-status**

username *<username>* **password** *<password>*

Use the **username password** command to configure the user name and password of the peer to use for Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured user name and password.

Syntax Description

<username>	Specifies a user name by alphanumerical string up to 30 characters in length (the user name is case sensitive).
<password>	Specifies a password by alphanumerical string up to 30 characters in length (the password is case sensitive).

Default Values

By default, there is no established user name and password.

Command History

Release 1.1	Command was introduced.

Functional Notes

Password Authentication Protocol (PAP) uses this entry to check received information from the peer. Challenge-Handshake Authentication Protocol (CHAP) uses this entry to check the received peer host name and a common password.

Usage Examples

The following example creates a user name of **Adtran** with password **Adtran** for the PPP link labeled 5:

(config)**#interface ppp 5**
(config-ppp 5)**#username Adtran password Adtran**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the Point-to-Point Protocol (PPP) 1 interface to the VRF instance named **RED**:

(config)**#interface ppp 1**
(config-ppp 1)**#vrf forwarding RED**

TUNNEL INTERFACE COMMAND SET

There are three different types of tunnel interfaces that can be configured in AOS. Generic routing encapsulation (GRE) tunnel interfaces, multipoint GRE (mGRE) tunnel interfaces, and virtual extensible local area network (VxLAN) interfaces.

The GRE tunnel interface creates a virtual point-to-point link between routers in an Internet Protocol (IP) network by encapsulating the IP packets first in a GRE packet (by adding a GRE header), then in an IP version 4 (IPv4) packet (by adding an IPv4 header). When the packets reach the terminating endpoint router, they are stripped of the IPv4 and GRE headers to reveal the packet payload.

This encapsulation process allows network routers to tunnel IPv4 traffic over an IPv4 network and IPv6 traffic over an IPv4 Internet connection (IPv6 over IPv4 GRE). For example, a host on an IPv6 network cannot normally communicate with a host on another IPv6 network using an IPv4 Internet connection. However, when using the GRE tunnel interface, the IPv6 packet is first encapsulated into a GRE packet, and the GRE traffic is then encapsulated into an IPv4 packet between the two tunnel endpoints. The terminating tunnel endpoint then removes the IPv4 and GRE headers, revealing the original IPv6 packet before sending it on to the destination host.

MGRE tunnel interfaces create a virtual multipoint link between routers in a Dynamic Multipoint Virtual Private Network (DMVPN), much the same way as GRE tunnel interfaces operate in an IP network. When you create a tunnel interface, you must specify whether the tunnel is a GRE tunnel or an mGRE tunnel.

VxLAN tunnel interfaces are used to expand Layer 2 network segments beyond physical network boundaries, utilizing Layer 3 as a underlay network. For example, to share computer resources, virtual machines (VMs) residing on physical servers in two separate locations must be able to transparently see a single Layer 2 network segment between each other.

VxLAN tunnel implementation is point-to-point only since AOS does not currently support multicast VxLAN tunnels. VxLAN tunnel support is limited to IPv4 for underlay networks. However, IPv6 overlay networks can be created over IPv4 underlay networks.

*Not all platforms have mGRE or VxLAN tunnel interfaces available. To see if your unit has this capability, type **show interfaces** at the enable prompt.*

To activate the GRE Tunnel Interface Configuration mode, enter the **interface tunnel** <*interface id*> **gre ip** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface tunnel 1 gre ip
(config-tunnel 1)#
```

To activate the mGRE Tunnel Interface Configuration mode, enter the **interface tunnel** <*interface id*> **multipoint-gre ip** command at the Global Configuration mode prompt. For example:

>enable
#configure terminal
(config)**#interface tunnel 1 multipoint-gre ip**
(config-tunnel 1)**#**

To activate the VxLAN Tunnel Interface Configuration mode, enter the **interface tunnel** <*interface id*> **vxlan** command at the Global Configuration mode prompt. For example:

>enable
#configure terminal
(config)**#interface tunnel 1 vxlan**
(config-tunnel 1)**#**

*Not all tunnel interface commands apply to all tunnel interface types. Use the **?** command to display a list of valid commands. For example:*

*>**enable***
*Password:**xxxxx***
#config term
*(config)#**interface tunnel 1 gre ip***
*(config-tunnel 1)#**?***
alias - A text name assigned by an SNMP NMS
bandwidth - Set bandwidth parameter
etc.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bandwidth <value> on page 3214
dial-backup commands begin on page 3215
dynamic-dns on page 3232
encapsulate-inner-vlan on page 3234
ip commands begin on page 3235
ipv6 commands begin on page 3284

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view the default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 9.1	Command was expanded to include the tunnel interfaces.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface.

Usage Examples

The following example sets bandwidth of the tunnel 1 interface to **10** Mbps:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#bandwidth 10000**

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the interface to automatically attempt a dial backup upon failure. Use the **no** form of this command to disable this feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3218*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial backup upon a failure.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example enables automatic dial backup on the endpoint:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup auto-backup**

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3218*.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to automatically restore the primary connection when the failure condition clears:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup auto-restore**

dial-backup backup-delay *<value>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3218*.

Syntax Description

<value>	Specifies the delay period (in seconds) a failure must be active before AOS will enter backup operation on the interface. Range is **10** to **86400** seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **60** seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup backup-delay 60**

dial-backup call-mode

Use the **dial-backup call-mode** command to specify whether the configured backup interface answers or originates (or a combination of both) backup calls. Use the **no** form of this command to return to the default value. Variations of this command include:

dial-backup call-mode answer
dial-backup call-mode answer-always
dial-backup call-mode originate
dial-backup call-mode originate-answer
dial-backup call-mode originate-answer-always

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer**.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Functional Notes

The majority of the configuration for AOS dial-backup implementation is configured via the dial-backup PPP interface configuration commands. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname “Remote3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.1.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
```



```
 coding b8zs
 framing esf
 clock source line
 tdm-group 1 timeslots 1-24
 no shutdown
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.16 point-to-point
 frame-relay interface-dlci 16
 ip address 10.1.1.2 255.255.255.252
 dial-backup call-mode originate
 dial-backup number 5551111 analog ppp1
 dial-backup number 5552222 analog ppp1
no shutdown
!
interface ppp 1
 ip address 172.22.56.1 255.255.255.252
 ppp authentication chap
 username remoterouter password remotepass
 ppp chap hostname localrouter
 ppp chap password adtran
 no shutdown
!
ip route 192.168.2.0 255.255.255.0 172.22.56.2 255.255.255.252
!
line telnet 0 4
 password password
```

Sample configuration for central router (dialing in)

```
hostname “Central3200”
enable password adtran
!
interface eth 0/1
 ip address 192.168.100.254 255.255.255.0
 no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
 coding b8zs
 framing esf
 clock source line
```



```
 tdm-group 1 timeslots 1-24
 no shutdown
!
interface fr 1 point-to-point
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.100 point-to-point
 frame-relay interface-dlci 100
 ip address 10.1.1.1 255.255.255.252
 dial-backup call-mode answer
 dial-backup number 555-8888 analog ppp 1
!
interface ppp 1
 ip address 172.22.56.2 255.255.255.252
 ppp authentication chap
 username localrouter password adtran
 ppp chap hostname remoterouter
 ppp chap password remotepass
 no shutdown
!
ip route 192.168.1.0 255.255.255.0 172.22.56.1 255.255.255.252

line telnet 0 4
 password password
```

Usage Examples

The following example configures AOS to generate backup calls for this endpoint using an analog modem interface (to phone number 555 1111), but never answer calls and specifies **ppp 2** as the backup interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup call-mode originate**
(config-tunnel 1)**#dial-backup number 555 1111 analog ppp 2**

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial backup, where in the configuration AOS accesses specific routing information, etc.):

Dialing Out

1. AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number on page 3225*).
3. When placing the call, AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, AOS places a call to the second number (if a second number is configured). The second number to be dialed references a separate PPP interface.

Dialing In

1. AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from caller ID, the call is terminated.

dial-backup connect-timeout <*value*>

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3218*.

Syntax Description

<*value*>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call. Valid range is **10** to **300** seconds.

Default Values

By default, the **dial-backup connect-timeout** period is set to **60** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **120** seconds before retrying a failed dial-backup call:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup connect-timeout 120**

dial-backup force

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3218*. Variations of this command include:

dial-backup force backup
dial-backup force primary

Syntax Description

backup	Force backup regardless of primary link state.
primary	Force primary link regardless of its state.

Default Values

By default, this feature is disabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to force this interface into dial backup:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup force backup**

dial-backup maximum-retry <*value*>

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode on page 3218*.

Syntax Description

<*value*>	Selects the number of call retry attempts that will be made after a link failure. Valid range is **0** to **15** attempts. Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to **0** attempts.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to retry a dial-backup call **four** times before considering backup operation not available:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup maximum-retry 4**

dial-backup number

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3218*. Variations of this command include:

dial-backup number <*number*> **analog ppp** <*interface*>
dial-backup number <*number*> **digital-56k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>
dial-backup number <*number*> **digital-64k** <*isdn min chan*> <*isdn max chan*> **ppp** <*interface*>

Syntax Description

<*number*>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates the number connects to an analog modem.
digital-56k	Indicates the number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates the number belongs to a digital 64 kbps per DS0 connection.
<*isdn min chan*>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection. Range is **1** to **24**.
<*isdn max chan*>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection. Range is **1** to **24**.
ppp <*interface*>	Specifies the Point-to-Point Protocol (PPP) interface to use as the backup for this interface.

Default Values

By default, there are no configured dial-backup numbers.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.
Release 17.2	Command was expanded to include the cellular connections.
Release 17.3	Cellular connections were removed from this command.

Usage Examples

The following example configures AOS to dial **704-555-1212** (digital 64 kbps connection) to initiate dial-backup operation on this endpoint using interface **ppp 1** backup interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup number 7045551212 digital-64k 1 1 ppp 1**

dial-backup priority <*value*>

Use the **dial-backup priority** command to select the backup priority for this interface. This allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3218*.

Syntax Description

<*value*>	Sets the relative priority of this link. Valid range is **0** to **100**. A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to **50**.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example assigns the highest priority to this endpoint:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup priority 100**

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3218*.

Syntax Description

No subcommands.

Default Values

By default, AOS does not randomize the dial-backup call timers.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to randomize the dial-backup timers associated with this endpoint:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup randomize-timers**

dial-backup redial-delay <*value*>

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3218*.

Syntax Description

<*value*>	Specifies the delay in seconds between attempting to redial a failed backup attempt. Range is **10** to **3600** seconds.

Default Values

By default, **dial-backup redial-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures a redial delay of **25** seconds on this endpoint:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup redial-delay 25**

dial-backup restore-delay *<value>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is bouncing in and out of alarm. Use the **no** form of this command to return to the default setting. For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3218*.

Syntax Description

<value>	Specifies the number of seconds AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range is **10** to **86400** seconds.

Default Values

By default, **dial-backup restore-delay** is set to **10** seconds.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example configures AOS to wait **30** seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup restore-delay 30**

dial-backup schedule

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial backup (as specified). For more detailed information on dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3218*. Variations of this command include:

dial-backup schedule day <*name*>
dial-backup schedule enable-time <*value*>
dial-backup schedule disable-time <*value*>

Syntax Description

day <*name*>	Sets the days to allow backup. Valid range is Monday through Sunday.
enable-time <*value*>	Sets the time of day to enable backup. Time is entered in a 24-hour format (00:00).
disable-time <*value*>	Sets the time of day to disable backup. Time is entered in a 24-hour format (00:00).

Default Values

By default, dial backup is enabled for all days and times if the **dial-backup auto-backup** command has been issued and the dial-backup schedule has not been entered.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Point-to-Point Protocol (PPP) interface.

Usage Examples

The following example enables dial backup Monday through Friday 8:00 a.m. to 7:00 p.m.:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup schedule enable-time 08:00**
(config-tunnel 1)**#dial-backup schedule disable-time 19:00**
(config-tunnel 1)**#no dial-backup schedule day Saturday**
(config-tunnel 1)**#no dial-backup schedule day Sunday**

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on Point-to-Point Protocol (PPP) dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode on page 3218*.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are **disabled**.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example deactivates the configured dial-backup interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dial-backup shutdown**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background and provides layout and functionality similar to a BIND zone file, allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates; however, updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#dynamic-dns dyndns-custom host user pass**

encapsulate-inner-vlan

Use the **encapsulate-inner-vlan** command to configure a virtual extensible local area network (VxLAN) interface to preserve the VLAN tag in Layer 2 frames transmitted via the VxLAN tunnel. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, the VxLAN tunnel strips the VLAN tag off of Layer 2 frames.

Command History

Release 13.1.0	Command was introduced.

Usage Examples

The following example enables preservation of the VLAN tag for VxLAN tunnel interface 1:

(config)**#interface tunnel 1 vxlan**
(config-tunnel 1)**#encapsulate-inner-vlan**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to create an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Assigns an IPv4 ACL name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the unit to only allow Telnet traffic (as defined in the user-configured **TelnetOnly** IP ACL) into the tunnel interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip access-policy PRIVATE**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface. Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 5.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures an IPv4 address of **192.22.72.101 255.255.255.252**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip address 192.22.72.101 255.255.255.252**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

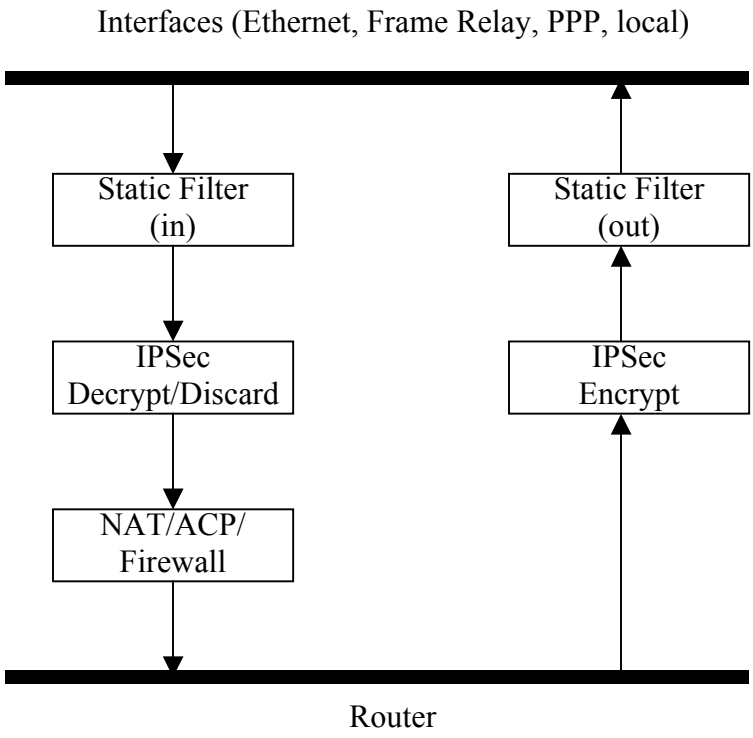
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip crypto map MyMap**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the VLAN, PPP, HDLC, BVI, demand, and loopback interfaces as well as the Ethernet, Frame Relay, and ATM subinterfaces.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644) with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **tunnel 1**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 4 (IPv4) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries to be cleared from this IPv4 interface.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.4.0	Maximum number of stored entries was expanded to **500000** and RapidRoute is now enabled by default.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv4 interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#no ip ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on a **tunnel** interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper-address** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248 /30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.

Syntax Description

query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.
static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 7.1	Command was introduced.
Release 8.1	Asynchronous transfer mode (ATM) subinterface was added.
Release 9.1	tunnel subinterface was added.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface and to place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 3256* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip mcast-stub downstream**

ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the command **ip igmp static-group** <*address*> (refer to *ip igmp on page 3250*) to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled, and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 3253*, and *ip mcast-stub upstream on page 3256* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled, and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 3253* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip mtu 1200**

ip nhrp authentication <*string*>

Use the **ip nhrp authentication** command to specify the authentication string used on the router for Next Hop Resolution Protocol (NHRP) communication in a Dynamic Multipoint Virtual Private Network (DMVPN) network. Use the **no** form of this command to disable NHRP authentication.

Syntax Description

<*string*>	Specifies a text string used for NHRP authentication. Strings should be no longer than **8** characters.

Default Values

By default, NHRP authentication is disabled.

Command History

Release R11.7.0	Command was introduced.

Functional Notes

The NHRP authentication string is used for NHRP communication and all routers communicating with NHRP must be configured with the same authentication string. The string is not encrypted.

Usage Examples

The following example configures an NHRP authentication string on tunnel interface **1**:

(config)**#tunnel interface 1 gre ip**
(config-tunnel 1)**#ip nhrp authentication STRINGX**

ip nhrp holdtime <*value*>

Use the **ip nhrp holdtime** command to specify how often the router sends Next Hop Resolution Protocol (NHRP) registration requests to the next-hop server (NHS). Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time, in seconds, between sending registration requests. Valid range is **1** to **65535** seconds.

Default Values

By default, the hold time is set to **7200** seconds. In addition, by default, the NHRP registration requests are sent at intervals of one third the hold time value; for example, if the hold time is set to 7200 seconds (default), then the registration requests are sent every 2400 seconds.

Command History

Release R11.7.0	Command was introduced.

Usage Examples

The following example specifies a hold time of **800** seconds on tunnel interface **1**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip nhrp holdtime 800**

ip nhrp map *<destination ipv4 address> <nbma address>*

Use the **ip nhrp map** command to statically create a Next Hop Resolution Protocol (NHRP) mapping between the Internet Protocol version 4 (IPv4) address and the nonbroadcast multiaccess (NBMA) address of the next hop server (NHS). Use the **no** form of this command to remove the mapping.

Syntax Description

<destination IPv4 address>	Specifies the destination IPv4 address to map to the NBMA address. Express IPv4 addresses in dotted decimal notation; for example, **10.10.10.1**.
<nbma address>	Specifies the NBMA address to map to the destination IPv4 address. Express the NBMA address in dotted decimal notation; for example, **192.168.1.101**.

Default Values

By default, no mapping is configured.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

In Dynamic Multipoint Virtual Private Networking (DMVPN), the destination IPv4 address is typically the private tunnel address, and the NBMA address is the tunnel's public facing address.

Usage Examples

The following example statically maps between the IPv4 destination address **10.10.10.1** and the NBMA address **192.168.1.101** on the unit:

(config)**#interface tunnel 1 multipoint-gre ip**
(config-tunnel 1)**#ip nhrp map 10.10.10.1 192.168.1.101**

ip nhrp map multicast *<nbma address>*

Use the **ip nhrp map multicast** command to statically add a Next Hop Resolution Protocol (NHRP) mapping for multicast and broadcast traffic to a nonbroadcast multiaccess (NMBA) address. The next-hop server (NHS) is typically used as the NBMA address. Use the **no** form of this command to remove the mapping.

Syntax Description

<nbma address>	Specifies the NBMA address that will receive multicast and broadcast traffic. This address is typically the NHS. Express NBMA addresses in dotted decimal notation; for example, **192.168.1.101**.

Default Values

By default, the NBMA address is not mapped.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

In Dynamic Multipoint Virtual Private Networking (DMVPN), the NBMA address is the tunnel's public facing address.

Usage Examples

The following example enables multicast and broadcast traffic to the NMBA address **192.168.1.101**:

(config)**#interface tunnel 1 multicast-gre ip**
(config-tunnel 1)**#ip nhrp map multicast 192.168.1.101**

ip nhrp nhs *<ip address>*

Use the **ip nhrp nhs** command to specify the address used by the router acting as a next-hop client (NHC) to communicate with the next-hop server (NHS) in a Dynamic Multipoint Virtual Private Network (DMVPN) configuration using Next Hop Resolution Protocol (NHRP). This address is the private tunnel address used in a Generic Routing Encapsulation (GRE) tunnel between the spoke (NHC) and the hub (NHS). Use the **no** form of this command to remove the address from the tunnel's configuration.

Syntax Description

<ip address>	Specifies the private tunnel IP address on the NHS. Specify IP addresses in dotted decimal notation (**10.10.10.1**).

Default Values

By default, no NHS address is configured.

Command History

Release R11.7.0	Command was introduced.

Functional Notes

Only a single address can be configured for a point-to-point GRE tunnel.

Usage Examples

The following example specifies an NHS address of **10.10.10.1** on tunnel interface **1**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip nhrp nhs 10.10.10.1**

ip nhrp record

Use the **ip nhrp record** command to specify whether Next Hop Resolution Protocol (NHRP) requests and replies should include forward and backward record extensions. Use the **no** form of this command to disable the addition of these extensions.

Syntax Description

No subcommands.

Default Values

By default, both forward and backward record extensions are included in NHRP requests and replies.

Command History

Release R11.9.0	Command was introduced.

Usage Examples

The following example disables the addition of forward and backward record extensions for NHRP messages:

(config)**#interface tunnel 1 multicast-gre ip**
(config-tunnel 1)**#no ip nhrp record**

ip nhrp registration non-unique

Use the **ip nhrp registration non-unique** command to specify whether the Unique flag is set in the Next Hop Resolution Protocol (NHRP) registration packet. Use the **no** form of this command to remove the Unique flag.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

The Generic Routing Encapsulation (GRE) tunnel source is used in NHRP registration events. When the source IP address changes, a new registration with the next hop server (NHS) occurs. Adtran recommends enabling the **ip nhrp registration non-unique** feature on interfaces where the IP addresses can change.

Usage Examples

The following example enables the Unique flag for NHRP registration packets on the interface:

(config)**#interface tunnel 1 multicast-gre ip**
(config-tunnel 1)**#ip nhrp registration non-unique**

ip nhrp registration timeout <*value*>

Use the **ip nhrp registration timeout** command to specify how often the router sends Next Hop Resolution Protocol (NHRP) registration requests to the next-hop server (NHS) independent of the NHRP hold time setting (refer to the command *ip nhrp holdtime <value> on page 3260*). Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time, in seconds, between NHRP registration requests. Valid range is **1** to **65535** seconds.

Default Values

By default, this option is not configured and the registration requests are sent at intervals of one third the hold time value (refer to the command *ip nhrp holdtime <value> on page 3260*).

Command History

Release R11.7.0	Command was introduced.

Functional Notes

The timeout value must be set to less than or equal to the value set with **ip nhrp holdtime** command.

Usage Examples

The following example specifies that NHRP registration requests are sent independently from the hold time value every **300** seconds:

(config)**#tunnel interface 1 gre ip**
(config-tunnel 1)**#ip nhrp registration timeout 300**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the tunnel interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include the tunnel interfaces.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip ospf 1 network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the tunnel 1 interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the tunnel 1 interface every **3600** seconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the neighbor timeout to **300** seconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation delay to **300** milliseconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 9.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the tunnel interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP **version 1** (the default value for the **version** command).

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the tunnel interface to accept only RIP version 2 packets:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP **version 1** (the default value for the **version** command).

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the tunnel interface to transmit only RIP version 2 packets:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 9.1	Command was introduced.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the tunnel interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip route-cache**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the tunnel interface and matches the URL filter named **MyFilter**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on an interface. Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the interface.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the interface.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the interface to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the interface.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an interface when other unicast IPv6 addresses are not needed on the interface. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the interface.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6**

ipv6 access-group *<ipv6 acl name>*

Use the **ipv6 access-group** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to be used for IPv6 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ipv6 access-group <*ipv6 acl name*> **in**
ipv6 access-group <*ipv6 acl name*> **out**

Syntax Description

<ipv6 acl name>	Applies the named IPv6 ACL to the interface.
in	Enables access control on IPv6 packets received on the specified interface.
out	Enables access control on IPv6 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 18.1	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Only one IPv6 ACL can be applied in each traffic direction.

Unlike in IPv4, IPv6 traffic filters include an implicit **permit** for neighbor solicitation and advertisement packets in an ACL before the traditional implicit **deny** at the end of the ACL. This prevents blocking of address resolution and unreachability detection, although this can be overridden by entering explicit **deny** commands in the IPv6 ACL.

Usage Examples

The following example applies the IPv6 ACL **Privatev6** to incoming IPv6 traffic on the interface:

(config)**#tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 access-group Privatev6 in**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3288*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3288*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the interface and enables IPv6 processing on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address <*ipv6 link-local address*> link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<*ipv6 link-local address*>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the interface.

Default Values

By default, no IPv6 address is configured for the interface and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

A single link-local address can be manually configured on an interface. The lower 64 bits of the specified address become the Interface ID for the interface, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the interface and can be derived from the interface's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the interface.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example manually creates a link-local IPv6 address on the interface and enables IPv6 processing:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 address autoconfig

Use the **ipv6 address autoconfig** command to enable Internet Protocol version 6 (IPv6) processing on the interface, create a local-link IPv6 address for the interface, and allow the interface to automatically configure itself based on advertisements from other routers on the link. Use the **no** form of this command to remove all autoconfigured addresses, prefixes, and any resulting routes from the interface and also causes the interface to cease processing received router advertisements (RAs).Variations of this command include:

ipv6 address autoconfig
ipv6 address autoconfig default
ipv6 address autoconfig default metric <*value*>

Syntax Description

default	Optional. Specifies that the interface maintain a list of advertising routers that are willing to be IPv6 default routers.
metric <*value*>	Optional. Specifies the administrative distance for a default router maintained in the default router list. Range is **1** to **255**. Routes with lower administrative distance are favored.

Default Values

By default, no IPv6 addresses are configured for the interface and IPv6 processing is not enabled. When an IPv6 address is configured automatically, the administrative distance for default routers is **2** by default.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

When autoconfiguration is enabled, the interface listens for RA messages that tell the interface how it should be configured. The interface then creates addresses for advertised 64-bit prefixes with the A flag in the IPv6 address set using stateless address autoconfiguration (SLAAC). The addresses use the EUI-64 interface ID in the lower 64 bits of the address. A route type of *Connected* is added to the route table if the L flag on the prefix advertisement (on-link flag) is also set.

Usage Examples

The following example enables IPv6 processing on the interface, creates a link-local IPv6 address for the interface, and allows the interface to automatically configure itself for IPv6:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 address autoconfig**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname <*partial fqdn*>
ipv6 address dhcp hostname fqdn <*fqdn*>
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 3284*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 address 2001:DB8:1::1/64**
(config-tunnel 1)**#ipv6 address dhcp fqdn client@company.com**

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*

Use the **ipv6 address named-prefix** command to create an Internet Protocol version 6 (IPv6) address for the interface using the values in a named prefix. Use the **no** form of this command to remove the address from the interface. Variations of this command include:

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*
ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>* **eui-64**

Syntax Description

<prefix name>	Specifies the named prefix to use to create the address.
<ipv6 address/prefix-length>	Specifies the address portion appended to the named prefix to create a 128-bit host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
eui-64	Optional. Indicates that the interface ID is to be placed in the lower 64 bits of the address.

Default Values

By default, no IPv6 addresses are specified on the interface.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example creates an IPv6 address on the interface using the named prefix **PREFIX1**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 address named-prefix PREFIX1 2001:1:0:/48**

ipv6 crypto map *<name>*

Use the **ipv6 crypto map** command to associate Internet Protocol version 6 (IPv6) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

Syntax Description

<name>	Specifies the IPv6 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Only one IPv6 crypto map can be specified per interface, and the crypto map is applied within the virtual routing and forwarding (VRF) instance to which the interface belongs. To apply the IPv6 crypto map, the interface must have IPv6 enabled. In addition, the interface must have an IPv6 address of appropriate scope to allow connectivity to peer's addresses as specified in the crypto map's entries.

Usage Examples

The following example applies all IPv6 crypto maps with the name **MyMap** to the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6**
(config-tunnel 1)**#ipv6 crypto map MyMap**

ipv6 dhcp client information refresh minimum <*seconds*>

Use the **ipv6 dhcp client information refresh minimum** command to specify the minimum value the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the interface accepts as its information refresh timer. Use the **no** version of this command to return to the default setting.

Syntax Description

<*seconds*>	Specifies the refresh timer in seconds. Valid range is **600** to **3600** seconds.

Default Values

By default, the DHCPv6 client refresh timer is set to **600** seconds.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example specifies the DHCPv6 client refresh timer for the interface is **800** seconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 dhcp client information refresh minimum 800**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 dhcp client pd PREFIX1**

ipv6 dhcp relay destination <*ipv6 address*>

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination <*ipv6 address*>
ipv6 dhcp relay destination <*ipv6 address*> <*interface*>
ipv6 dhcp relay destination <*ipv6 address*> **mef-ethernet** <*slot/port*>
ipv6 dhcp relay destination <*ipv6 address*> **system-control-evc**
ipv6 dhcp relay destination <*ipv6 address*> **system-management-evc**

Syntax Description

<*ipv6 address*>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*interface*>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the <*interface type*> <*slot/port* | *interface id*> format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** <*ipv6 address*> **?** to display a list of valid interfaces.
mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the system control Ethernet virtual connection (EVC) is used when sending messages to the DHCPv6 server.
system-management-evc	Optional. Specifies the system management EVC is used when sending messages to the DHCPv6 server.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command *ipv6 on page 3284*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6**
(config-tunnel 1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped mulitcast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the interface and specify that the interface is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the interface, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the interface. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this interface. All DHCPV^ requests received on this interface are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Enabling the interface as a DHCPv6 server using this command places the interface into DHCPv6 server mode. DHCPv6 modes (server or relay) are mutually exclusive at the interface. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the interface as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 address 2001:DB8:1::1/64**
(config-tunnel 1)**#ipv6 dhcp server POOL1**

ipv6 ffe

Use the **ipv6 ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 6 (IPv6) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 ffe
ipv6 ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries to be cleared from this IPv6 interface.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled on IPv6-enabled interfaces (using the command *ipv6 on page 2231*). The default number of **max-entries** is **4096**.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv6 interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#no ipv6 ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the interface in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the interface.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the interface in host mode:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 mode host unicast**

ipv6 mtu *<size>*

Use the **ipv6 mtu** command to specify the maximum transmission unit (MTU) for Internet Protocol version 6 (IPv6) packets on the interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Specifies the MTU value. Valid range is **1280** to **1500** bytes.

Default Values

By default, the MTU of the interface is set to **1280** bytes.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

In IPv6, the minimum MTU is 1280 octets. Any link that has an MTU less than 1280 octets must use link fragmentation and reassembly that is transparent to IPv6 (for example, the Fragmentation Header). Sources in the IPv6 network are expected to perform path maximum transmission unit (PMTU) discovery to send packets larger than 1280 octets. PMTU works in the following manner: First, the sending node assumes the link MTU of the interface from which the traffic is being forwarded and then sends the IPv6 packet at the link MTU size. If a router on the path is unable to forward the packet, it sends an ICMP *Packet Too Big* message back to the sending node containing the link MTU of the link on which the packet forwarding failed. The sending node then rests the PMTU to the value of the MTU field in the Internet Control Message Protocol version 6 (ICMPv6) *Packet Too Big* message, and the packet is resent.

The MTU for IPv6 packets can be set on a per-interface basis. There are two methods for setting MTUs for interfaces if required: one for Layer 3 interfaces, and one for the underlying Layer 1 and Layer 2 interfaces. For all interface types, use the **ipv6 mtu** *<size>* command to specify the IPv6 MTU in bytes from the interface's configuration mode. The minimum MTU setting for IPv6 is **1280** bytes, and the maximum is **1500** bytes. The IPv6 MTU value is independent of the IPv4 MTU setting (set with the command *ip mtu <size> on page 3257*).

When the interface is forwarding the IPv6 packet as a router, if the packet size exceeds the IPv6 MTU of the egress interface, the packet is dropped and ICMPv6 *Packet Too Big* message is sent to the source. When originating an IPv6 packet from the local IPv6 stack, and the packet is larger than the IPv6 MTU of the egress interface, the packet is fragmented and sent.

Usage Examples

The following example specifies the IPv6 MTU value for the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 mtu 1350**

ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** command to specify that the Advertisement Interval Option is sent in Internet Protocol version 6 (IPv6) router advertisement (RA) messages from the router. This command is effectual only when the interface is in router mode. Use the **no** form of this command to return to the default interval.

Syntax Description

No subcommands.

Default Values

By default, Advertisement Interval Options are not sent in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

Sending the Advertisement Interval Option should be enabled when the router is functioning in a mobile IP environment to aid movement detection by mobile nodes. This option contains the current value of the maximum router advertisement interval configured using the command *ipv6 nd ra interval on page 3314*.

Usage Examples

The following example specifies that the interface include Advertisement Interval Options in RA messages sent from the router:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd advertisement-interval**

ipv6 nd cache max-incomplete <*number*>

Use the **ipv6 nd cache max-incomplete** command to specify the maximum number of incomplete entries the Neighbor Discovery (ND) cache retains. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of incomplete ND entries to retain in the cache. Valid range is **1** to **321**.

Default Values

By default, the incomplete ND entries can take at maximum one-third of the possible ND cache entries (varies by product).

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example specifies that the interface stores **150** incomplete entries in the ND cache:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd cache max-incomplete 150**

ipv6 nd dad attempts *<number>*

Use the **ipv6 nd dad attempts** command to specify the number of neighbor solicitation (NS) messages sent by the interface when performing Internet Protocol version 6 (IPv6) duplicate address detection (DAD). This command is effectual when the interface is in either host or router mode. Use the **no** form of this command to return to the default value.

Syntax Description

<number>	Specifies the number of NS messages that will be sent. Range is **0** to **10** messages. A value of **0** disables DAD on the interface.

Default Values

By default, the interface sends **1** NS message.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

DAD is used by devices to determine if IPv6 addresses are unique before they are applied to interfaces. DAD is used in NS messages to detect duplicate unicast addresses. The Target Address fields in the NS messages are set to the IPv6 address for which duplication is being detected. Destination IPv6 addresses for DAD in NS messages are the solicited-node multicast version of the address being tested. Source IPv6 addresses for DAD are set to the IPv6 unspecified address (::). Once the IPv6 address is determined by DAD to be unique, it can be applied to the IPv6 interface on the node.

DAD in AOS is performed when an interface transitions state from DOWN to UP or when manually configuring an address. When performing DAD because of an interface transition, DAD will happen immediately after the interface transition and again 40 seconds later to cooperate with the port being connected to an Ethernet switch.

Usage Examples

The following example specifies that **3** NS messages are sent by the interface when performing DAD:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd dad attempts 3**

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command to specify the M flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. The M flag instructs hosts receiving the RA that they can use stateful Dynamic Host Configuration Protocol version 6 (DHCPv6) to configure addresses and nonaddress information. Use the **no** form of this command to disable the setting of the M flag.

Syntax Description

No subcommands.

Default Values

By default, the M flag is not set in RAs.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

If you specify that the M flag is set in RA messages, you do not need to set the 0 flag (it becomes redundant).

Usage Examples

The following example sets the M flag for RA messages sent by the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd managed-config-flag**

ipv6 nd ns-interval *<value>*

Use the **ipv6 nd ns-interval** command to specify the interval between transmission of certain Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages and to control what ND value is advertised in router advertisement (RA) messages. This command is effectual whether the interface is in host or router mode. Use the **no** form of this command to return the interval to the default value.

Syntax Description

<value>	Specifies the time (in milliseconds) between neighbor message transmissions. Valid range is **1000** to **3600000** ms.

Default Values

By default, the interval is set to **1000** ms for internal use by the router and **0** (unspecified) is sent in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

This command controls the spacing of NS messages for functions such as address resolution, reachability detection, and DAD. For DAD it also serves as the amount of time after the last transmission before the detection phase of autoconfiguration terminates. In addition, the command controls the interval between unsolicited NA messages.

Usage Examples

The following example changes the interval between RA messages sent from the interface to **2000** ms:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd ns-interval 2000**

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command to specify the O flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. When the O flag is set, hosts receiving the RA messages are instructed that they may use stateless Dynamic Host Configuration Protocol version 6 (DHCPv6) to receive information that is not IPv6 addressing information, and to use some other method (whether through manual configuration, stateless address autoconfiguration (SLAAC), etc.) for addressing information. Use the **no** form of this command to disable the O flag setting.

Syntax Description

No subcommands.

Default Values

By default, the O flag is not set in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

If the M flag is set for RA messages, you do not need to set the O flag.

Usage Examples

The following example sets the O flag in RA messages from the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd other-config-flag**

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the interface. Use the **no** form of this command to remove the specified prefix configuration from the interface. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the interface is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the interface. Prefixes for IPv6 addresses configured on a router interface are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the interface.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the interface:

(config)**#interface tunnel 1**
(config-tunnel 1)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ipv6 nd purge-timer <*value*>

Use the **ipv6 nd purge-timer** command to specify the maximum amount of time an unused Internet Protocol version 6 (IPv6) neighbor entry remains in the neighbor cache. This command applies to interfaces in either host or router mode. Use the **no** form of this command to return the purging interval to the default value.

Syntax Description

<*value*>	Specifies the neighbor cache entry storage time in minutes. Valid range is **10** to **1440** minutes.

Default Values

By default, idle (STALE) neighbor cache entries are cleared after **1440** minutes (24 hours).

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

This command applies to interfaces in either router or host mode. A neighbor entry is typically purged when neighbor unreachability detection (NUD) is invoked and the neighbor is determined to no longer be reachable. However, NUD is not performed on idle (STALE) neighbor entries, so this command provides a method for purging unused entries after a specified amount of time.

Usage Examples

The following example specifies that idle neighbor entries in the neighbor cache are removed after **800** minutes:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd purge-timer 800**

ipv6 nd ra interval

Use the **ipv6 nd ra interval** command to specify the interval between transmission of Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 nd ra interval *<max time>*
ipv6 nd ra interval *<max time> <min time>*
ipv6 nd ra interval msec *<max time>*
ipv6 nd ra interval msec *<max time> <min time>*

Syntax Description

<max time>	Specifies the maximum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **4** to **1800** seconds and **70** to **1800000** ms.
<min time>	Optional. Specifies the minimum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **3** seconds to 75 percent of the configured maximum time value in seconds, or **30** ms to 75 percent of the configured maximum time value in ms.
msec	Optional. Specifies that the time values are in milliseconds.

Default Values

By default, the interval is set in seconds and has a maximum interval time of **200** seconds and a minimum interval time of 75 percent of the maximum seconds value, but not less than **3** seconds.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

If this router is used as a default router, the interval between RA messages should not be set to a larger value than the RA lifetime set by the command *ipv6 nd ra lifetime <value> on page 3315*, which has a default value of **1800** seconds.

Usage Examples

The following example specifies that the maximum interval in seconds between RA message transmissions is **300**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd ra interval 300**

ipv6 nd ra lifetime <*value*>

Use the **ipv6 nd ra lifetime** command to specify the router lifetime advertised in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is effectual when the interface is in router mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

ipv6 nd ra lifetime <*value*>
ipv6 nd ra lifetime default-route

Syntax Description

<*value*>	Specifies the router lifetime in seconds. Range is **0** to **9000** seconds. A value of **0** indicates this is not a default router. A value other than 0 indicates to other nodes that this router can be used as a default router.
default-route	Specifies the RA lifetime is **0** if no default route exists on any IPv6 interface.

Default Values

By default, the router lifetime is set to **1800** seconds.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R11.5.0	Command was expanded to include the **default-route** parameter.

Functional Notes

A value other than **0** for a router lifetime should be larger than the router advertisement interval specified in the command *ipv6 nd ra interval on page 3314*.

Usage Examples

In the following example, the router lifetime advertised in RA messages is **3000** seconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd ra lifetime 3000**

ipv6 nd ra reachable-time <*value*>

Use the **ipv6 nd ra reachable-time** command to specify the value advertised for reachable time in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command also specifies the internal base reachable time used by the router. This command is effectual for interfaces in either host or router mode. Use the **no** form of this command to return the reachability value to the default setting.

Syntax Description

<*value*>	Specifies the reachability time in milliseconds. Range is **0** to **3600000** ms. A value of **0** indicates the reachable time is unspecified.

Default Values

By default, the router advertises a reachability time of **0** ms and uses an internal value of **30000** ms.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Functional Notes

This command is effectual for interfaces in either router or host mode. For hosts, this value sets the internal reachable time used by the host if no RAs are received specifying a different value. For routers, the value indicates the amount of time a device is considered reachable after having received a reachability confirmation in neighbor unreachabililty detection (NUD).

Usage Examples

The following example specifies that a reachability time of **50000** ms is advertised in RA messages:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd ra reachable-time 50000**

ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command to specify whether Internet Protocol version 6 (IPv6) router advertisement (RA) messages will be suppressed. This command only applies to interfaces in router mode. Use the **no** form of this command to begin sending RA messages.

Syntax Description

No subcommands.

Default Values

By default, RA messages are not suppressed. When IPv6 routing is not enabled on the router, or when implemented in a host-only mode, the default setting is to suppress advertisements on all interface types.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Usage Examples

The following example suppresses RA messages on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd ra suppress**

ipv6 nd router-preference

Use the **ipv6 nd router-preference** command to specify the default router preference value set in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. Setting this preference helps the receivers of RA messages to determine the preference of one router over another as a default router in environments with multiple routers. Use the **no** form of this command to return the preference to the default setting. Variations of this command include:

ipv6 nd router-preference high
ipv6 nd router-preference low
ipv6 nd router-preference medium

Syntax Description

high	Specifies the preference value is high.
low	Specifies the preference value is low.
medium	Specifies the preference value is medium.

Default Values

By default, the router preference is set to medium.

Command History

Release 18.1	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.

Usage Examples

The following example specifies that the advertised default router preference is high:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ipv6 nd router-preference high**

ipv6 route-cache

Use the **ipv6 route-cache** command to enable Internet Protocol version 6 (IPv6) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 18.2	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Fast switching allows an IPv6 interface to provide optimum performance when processing IPv6 traffic.

Usage Examples

The following example enables IPv6 fast switching on the interface:

(config)**#tunnel 1gre ip**
(config-tunnel 1)**#ipv6 route-cache**

keepalive

Use the **keepalive** command to periodically send keepalive packets to verify the integrity of the tunnel from end to end. Use the **no** form of this command to disable keepalives. Variations of this command include:

keepalive
keepalive <*value*>
keepalive <*value*> <*number*>

Syntax Description

<*value*>	Defines the time interval (in seconds) between transmitted keepalive packets. Valid range is **1** to **32767** seconds.
<*number*>	Defines the number of times to retry after failed keepalives before determining that the tunnel endpoint is down. Valid range is **1** to **255** times.

Default Values

By default, keepalives are disabled. When enabled, the keepalive period defaults to **10** seconds and the retry count defaults to **3** times.

Command History

Release 9.1	Command was introduced.

Functional Notes

Keepalives do not have to be configured on both ends of the tunnel in order to work. A tunnel is not aware of incoming keepalive packets.

Usage Examples

The following example enables **keepalive** with a period of **30** seconds and a retry count of **5** times:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#keepalive 30 5**

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the tunnel interface to receive LLDP packets:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to disable this feature. Variations of this command include:

lldp send
lldp send management-address
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

By default, all interfaces are configured to transmit and receive LLDP packets of all types.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the tunnel interface to transmit LLDP packets containing all enabled information types:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#lldp send**

The following example configures the tunnel interface to transmit and receive LLDP packets containing all information types:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#lldp send-and-receive**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip primary vrrp <*number*>
media-gateway ip primary vrrpv3 <*number*>
media-gateway ip secondary <*ipv4 address*>
media-gateway ip secondary vrrp <*number*>
media-gateway ip secondary vrrp <*number*> <*ipv4 address*>
media-gateway ip secondary vrrpv3 <*number*>
media-gateway ip secondary vrrpv3 <*number*> <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrrp <*number*>	Specifies that the IPv4 address of the Virtual Router Redundancy Protocol version 2 (VRRP) router group's virtual router ID (VRID) is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
vrrpv3 <*number*>	Specifies that the IPv4 address of the VRRP version 3 (VRRPv3) VRID is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
<*ipv4 address*>	Optional. Specifies a secondary IPv4 address of the VRRP or VRRPv3 VRID is used as the media gateway address on the interface. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A4.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.
Release R12.2.0	Command was expanded to include the **vrrp** and **vrrpv3** parameters.

Functional Notes

To use VRRP or VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRP or VRRPv3.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#media-gateway ip primary**

media-gateway ipv6

Use the **media-gateway ipv6** command to associate an Internet Protocol version 6 (IPv6) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv6 address associated with it. However, some interfaces allow dynamic configuration of IPv6 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ipv6
media-gateway ipv6 <*ipv6 address*>
media-gateway ipv6 loopback <*interface id*>
media-gateway ipv6 vrrpv3 <*number*>
media-gateway ipv6 vrrpv3 <*number*> <*ipv6 address*>

Syntax Description

<*ipv6 address*>	Specifies an IPv6 address to use for the media gateway. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
loopback <*interface id*>	Specifies an IPv6 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv6 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
vrrpv3 <*number*>	Specifies that all the secondary IPv6 addresses of the Virtual Routing Redundancy Protocol version 3 (VRRPv3) virtual router ID (VRID) are used as media gateway addresses on the interface. Valid VRID range is **1** to **255**.
<*ipv6 address*>	Optional. Specifies a single IPv6 address of the VRRPv3 VRID is used as the media gateway address on the interface. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

Default Values

By default, **media-gateway ipv6** is disabled.

Command History

Release R10.8.0	Command was introduced.
Release R12.2.0	Command was expanded to include the **vrrpv3** parameters.

Functional Notes

To use VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRPv3.

Usage Examples

The following example configures the unit to use the IPv6 address for RTP traffic:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#media-gateway ipv6**

mtu <*size*>

Use the **mtu** command to specify the maximum transmission unit (MTU) for a virtual extensible local area network (VxLAN) tunnel interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Specifies the MTU value. Valid range is **64** to **1464** bytes.

Default Values

By default, the MTU of the interface is set to 1464 bytes.

Command History

Release 13.1.0	Command was introduced.

Functional Notes

A VxLAN tunnel interface has two MTUs associated with it, one that is dynamically configured based on the outgoing IPv4 Ethernet interface (refer to the MTU specified by the *ip mtu <size> on page 3257*). The minimum value of these two MTUs is used when transmitting a packet from this tunnel interface. If an IP security (IPSec) profile has been applied to the tunnel, the MTU size may need to be reduced to accommodate a larger packet header.

Usage Examples

The following example specifies the MTU value for the VxLAN tunnel interface:

(config)**#interface tunnel 1 vxlan**
(config-tunnel 1)**#mtu 1350**

ospfv3 <*process id*> **area** <*area id*>

Use the **ospfv3 area** command to add an interface to an Open Shortest Path First version 3 (OSPFv3) process, and to configure the OSPFv3 process on the interface. This command places the interface in the specified area for the specified Internet Protocol version 6 (IPv6) OSPFv3 address family, and optionally defines the instance ID that is used to represent this OSPFv3 process in messages on the interface's link. Use the **no** form of this command to remove the OSPFv3 process from the interface. Variations of this command include:

ospfv3 <*process id*> **area** <*area id*> **ipv6**
ospfv3 <*process id*> **area** <*area id*> **ipv6 instance** <*instance id*>

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join, for the specified address family. The process ID is locally significant to the device, and must be unique among all OSPFv3 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the given OSPFv3 process. Valid range is **0** to **4294967295**.
ipv6	Identifies the OSPFv3 address family as IPv6.
instance <*instance id*>	Optional. Specifies the value to use in the instance ID field of messages sent or received by this OSPFv3 process on the interface's link. Valid range is **0** to **31**.

Default Values

By default, an OSPFv3 process is not configured on an interface. By default, process IDs, area IDs, and instance IDs are not defined.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

When using this command to enable an OSPFv3 process on an interface, keep the following rules in mind:

- The interface must have the address family enabled on the interface. If the address family is not enabled on the interface, the command is rejected and an error is displayed.
- Only interfaces on the default virtual routing and forwarding (VRF) instance support this command. Interfaces on a nondefault VRF will display an error when you attempt to configure OSPFv3 settings.
- The interface and the specified OSPFv3 process (if defined in the global configuration) must be in the same VRF or the command will fail.
- The address family must match that specified for the OSPFv3 process if the process has been defined in the global configuration or the command will fail.
- If the OSPFv3 process identified by the process ID does not exist in the global configuration, it is automatically created, along with the specified address family, and it is assigned to the VRF of which the interface is a member.

- If the specified OSPFv3 process is already at its maximum limit of processes or address families, the command fails.
- If the specified OSPFv3 process already exists in the global configuration, but its configuration does not include an address family, the specified address family is added to the OSPFv3 router configuration.
- A given OSPFv3 process can only have one address family.
- Multiple OSPFv3 instances per address family, per VRF, can be created and can be assigned to a given interface.
- If the interface's VRF changes, all OSPFv3 assignments are removed.
- To change an OSPFv3 process's VRF, the process must first be removed and then recreated. Removing the process removes all OSPFv3 assignments for that process form all interfaces.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To add an interface to the OSPFv3 process **5**, in area **10**, with an instance ID of **10**, enter the command as follows:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 5 area 10 ipv6 instance 10**

ospfv3 authentication

Use the **ospfv3 authentication** command to authenticate an interface that is performing Internet Protocol version 6 (IPv6) Open Shortest Path First version 3 (OSPFv3) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ospfv3 authentication ipsec spi <*spi*> **md5** <*key*>
ospfv3 authentication ipsec spi <*spi*> **sha1** <*key*>
ospfv3 authentication null

Syntax Description

ipsec	Specifies that IP security (IPsec) authentication is used.
spi <*spi*>	Specifies the security parameter index (SPI). Valid range is **256** to **4294967295**.
md5 <*key*>	Specifies that MD5 authentication is used. Keys are specified in 32 hexadecimal characters.
sha1 <*key*>	Specifies that SHA-1 authentication is used. Keys are specified in 40 hexadecimal characters.
null	Specifies that no OSPFv3 authentication is used.

Default Values

By default, this is set to **null** (meaning no authentication is used).

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example specifies that no OSPFv3 authentication will be used on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 authentication null**

ospfv3 *<process id>* **cost** *<cost>*

Use the **ospfv3 cost** command to specify a value that represents the cost of sending an Open Shortest Path First version 3 (OSPFv3) packet over the interface. Use the **no** form of this command to return the cost to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
cost *<cost>*	Specifies the OSPFv3 cost of the interface. This value overrides any automatically computed cost value (default value). Valid range is **1** to **65535**.

Default Values

By default, the OSPFv3 cost of the interface is automatically computed. The automatic cost computation is the reference bandwidth divided by the interface bandwidth. The reference bandwidth is set by the command *auto-cost reference-bandwidth <value> on page 4150*, and defaults to **100** Mbps.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the OSPFv3 cost of the interface as **10**:

```
(config)#interface tunnel 1 gre ip
(config-tunnel 1)#ospfv3 5 cost 10
```

ospfv3 <*process id*> dead-interval <*value*>

Use the **ospfv3 dead-interval** command to specify the maximum interval allowed between Open Shortest Path First version 3 (OSPFv3) Hello packets on the interface. If the maximum interval is exceeded, neighboring devices will assume that the device is down. This value must be the same across all interfaces on a link. Use the **no** form of this command to return the dead interval to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
dead-interval <*value*>	Specifies the maximum number of seconds allowed between OSPFv3 Hello packets. It is recommended that this value be **4** times the Hello packet interval (set with the command *ospfv3 <process id> hello-interval <value> on page 3336*). Valid range is **1** to **65535** seconds.

Default Values

By default, the maximum interval allowed between OSPFv3 Hello packets is set to **40** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To specify the dead interval between OSPFv3 Hello packets on the interface, enter the command as follows:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 5 dead-interval 100**

ospfv3 encryption

Use the **ospfv3 encryption** command to specify a symmetrical, bidirectional Open Shortest Path First version 3 (OSPFv3) security association (SA) that uses encapsulating security payload (ESP) for encryption and authentication of all OSPFv3 messages that are sent or received on the interface. This command allows you to specify OSPFv3 security at the interface level. Use the **no** form of this command to remove IP security (IPsec) protection of OSPFv3 messages on the interface. Variations of this command include:

ospfv3 encryption ipsec spi <*spi*> **esp** <*encryption type*> <*encryption key*> <*authentication type*> <*authentication key*>
ospfv3 encryption ipsec spi <*spi*> **esp null** <*authentication type*> <*authentication key*>
ospfv3 encryption null

Syntax Description

ipsec	Specifies that IPsec encryption is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by any other IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
esp	Specifies that ESP is used.
null	Specifies that OSPFv3 messages on this interface are not encrypted when used in the **ospfv3 encryption null** format (even when encryption is specified by the OSPFv3 area configuration). When used in the **ospfv3 encryption ipsec spi** <*spi*> **esp null** format, **null** indicates that messages on the interface will not be encrypted, but will be authenticated.
<*encryption type*>	Specifies the type of algorithm used to encrypt OSPFv3 messages. Valid values for encryption are: **3des** uses triple data encryption standard (DES). **aes-cbc** uses advanced encryption standard (AES) with cipher block chaining (CBC). Select from **aes-cbc 128**, **aes-cbc 192**, or **aes-cbc 256**. **des** uses DES.
<*encryption key*>	Specifies the hexadecimal encryption key. The size of the encryption key is determined by the respective encryption algorithm, as follows: **3des** uses a **48** character key size. **aes-cbc 128** uses a **32** character key size. **aes-cbc 192** uses a **48** character key size. **aes-cbc 256** uses a **64** character key size. **des** uses a **16** character key size.
<*authentication type*>	Specifies the algorithm used for authenticating OSPFv3 messages. Valid authentication methods are Message-Digest 5 (**md5**) and Secure-Hash 1 (**sha1**) algorithms.

<authentication key> Specifies the hexadecimal authentication key. The size of the authentication key is determined by the respective authentication algorithm, as follows:

md5 uses a **32** character key size.

sha1 uses a **40** character key size.

Default Values

By default, there is no security for OSPFv3 messages on an interface.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

This commands specifies OSPFv3 security at the interface level. Protection specified with this command overrides any area-level OSPFv3 protection that might apply to the interface.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages with an SPI of **120**, no encryption, and **md5** as the authentication method:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 encryption ipsec spi 120 esp null md5**
NeWtStpsswdLoonGpsswDhtThmnWoKEY

ospfv3 <*process id*> **hello-interval** <*value*>

Use the **ospfv3 hello-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) Hello packets sent on the interface. This value must be the same across all interfaces on the link. Use the **no** form of this command to return the Hello packet interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
hello-interval <*value*>	Specifies the number of seconds allowed between OSPFv3 Hello packets. Valid range is **1** to **65535** seconds.

Default Values

By default, the Hello packet interval for OSPFv3 is **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the interval between OSPFv3 Hello packets on the interface is **20** seconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 5 hello-interval 20**

ospfv3 <*process id*> network

Use the **ospfv3 network** command to specify the network type for Open Shortest Path First version 3 (OSPFv3) enabled interfaces. Use the **no** form of this command to return the interface's network type to the default value. Variations of this command include:

ospfv3 <*process id*> **network broadcast**
ospfv3 <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
broadcast	Specifies that the OSPFv3 network type for the interface is set to broadcast.
point-to-point	Specifies that the OSPFv3 network type for the interface is set to point-to-point.

Default Values

By default, Ethernet interfaces are set to network type broadcast, and point-to-point (PPP), Frame Relay, and loopback interfaces are set to network type point-to-point.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the network interface as point-to-point:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 5 network point-to-point**

ospfv3 *<process id>* **priority** *<value>*

Use the **ospfv3 priority** command to specify the Open Shortest Path First version 3 (OSPFv3) priority for the interface. Use the **no** form of this command to return the interface's priority to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
priority *<value>*	Specifies the OSPFv3 priority for the interface. Valid range is **0** to **255**.

Default Values

By default, the OSPFv3 priority of an interface is set to **1**.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

Priority is used in the election of the designated router and backup designated router on multi-access networks. Interfaces connected to multi-access networks (such as Ethernet interfaces) perform an election for a designated and backup designated router. The router interface with the highest OSPFv3 priority on the link becomes the designated router for that link. The interface with the next highest priority becomes the designated backup router. In the event there is a tie, the router interface with the highest router ID takes precedence. A priority value of **0** indicates the router is ineligible to become either the designated or backup designated router.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's OSPFv3 priority value to **6**:

```
(config)#interface tunnel 1 gre ip
(config-tunnel 1)#ospfv3 5 priority 6
```

ospfv3 <*process id*> retransmit-interval <*value*>

Use the **ospfv3 retransmit-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) sent on the interface. Use the **no** form of this command to return the OSPFv3 LSA interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
retransmit-interval <*value*>	Specifies the number of seconds between OSPFv3 LSAs sent on the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA retransmit interval is set to **5** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the LSA retransmit interval is **10** seconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 5 retransmit-interval 10**

ospfv3 <*process id*> shutdown

Use the **ospfv3 shutdown** command to disable an Open Shortest Path First version 3 (OSPFv3) process on the interface. When this command is used, the OSPFv3 commands remain in place, but logically it appears to the interface as though the OSPFv3 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv3 process.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables OSPFv3 process **5** on the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 5 shutdown**

ospfv3 <*process id*> transmit-delay <*value*>

Use the **ospfv3 transmit-delay** command to specify the estimated time that is required to propagate an Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) on the interface. Use the **no** form of this command to return the transmit delay to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3329*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
transmit-delay <*value*>	Specifies the number of seconds required to send LSAs from the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA transmit delay is set to **1** second.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's LSA transmit delay to **2** seconds:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ospfv3 5 transmit-delay 2**

packet-capture <*name*>

Use the **packet-capture** command to apply a previously configured packet capture instance to the interface. Use the **no** form of this command to remove the packet capture instance.

Syntax Description

<*name*>	Specifies the name of the packet capture instance to apply to the interface.

Default Values

By default, no packet capture instances are configured or applied to the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. For more information about packet capturing, its uses, and its implementation in AOS, refer to the configuration guide *Configuring Packet Capture in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example applies the previously configured packet capture **1CAPTURE** to the interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#packet-capture 1CAPTURE**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to police incoming or outgoing packets on the tunnel interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the system control Ethernet virtual connection (EVC) and system management EVC.
Release R11.9.0	Command was expanded to include the tunnel interface for policing QoS maps.

Functional Notes

When a QoS policy is applied to a tunnel interface, it is used to police the inbound or outbound traffic on the interface. QoS maps configured with information other than the traffic police rates and traffic matching criteria (set using the commands *match on page 4469* and *police cir <rate> on page 4479*) cannot be associated with the tunnel interface. Instead, the association between the QoS map and the tunnel interface is rejected.

Usage Examples

The following example applies the QoS map **QOSPOLICE1** to outbound traffic on the Tunnel interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#qos-policy out QOSPOLICE1**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP on the tunnel interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.2	Command was expanded to the cellular interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the tunnel interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#no snmp trap link-status**

tunnel checksum

Use the **tunnel checksum** command to verify the checksum of incoming generic routing encapsulation (GRE) packets and to include a checksum on outgoing packets. Use the **no** form of this command to disable checksum.

Syntax Description

No subcommands.

Default Values

By default, **tunnel checksum** is disabled.

Command History

Release 9.1	Command was introduced.

Functional Notes

Both ends of the tunnel must have **tunnel checksum** enabled in order for a meaningful configuration. When both endpoints have **tunnel checksum** enabled, a packet with an incorrect checksum will be dropped. If the endpoints differ in their checksum configuration, all packets will still flow without any checksum verification.

Usage Examples

The following example enables checksum on the tunnel 1 interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel checksum**

Technology Review

When enabled, the **tunnel checksum** will be calculated for each outgoing GRE packet with the result stored in the GRE header. The checksum present bit will also be set in the header.

tunnel destination *<ip address>*

Use the **tunnel destination** command to specify the IP address to use as the destination address for all packets transmitted on this interface. Use the **no** form of this command to clear the **tunnel destination** address.

Syntax Description

<ip address>	Specifies the IP address to use as the destination address for all packets transmitted on this interface. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no tunnel destinations are defined.

Command History

Release 9.1	Command was introduced.

Functional Notes

Until a tunnel interface has a destination IP address defined, it is not operational.

The tunnel destination IP address will be the value put into the destination field of the outer IP header after generic routing encapsulation (GRE) of the original packet. A route must be defined for the destination address. Be certain there are no recursive routes by ensuring that a tunnel's destination address will be routed out a physical interface. There is a possibility of creating a routing loop when tunnel interface traffic gets routed back to the same tunnel interface or to another tunnel interface, which in turn, does not have a route out of a physical interface. In either case, the tunnel will go down for a period of one minute, after which it will come back up to determine if the recursive routes have been resolved. This allows time for routing protocols to converge on a valid route. If a static route has caused the recursive routing loop, the tunnel status may oscillate until the route is changed.

Usage Examples

The following example sets the tunnel destination IP address to **192.22.73.101**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel destination 192.22.73.101**

tunnel key *<value>*

Use the **tunnel key** command to specify a value shared by both endpoints of the tunnel that will provide minimal security and delineate between tunnels with the same source and destination addresses. Use the **no** form of this command to disable the key.

Syntax Description

<value>	Defines the key value for this tunnel. Valid range is **1** to **4294967294**.

Default Values

By default, a key is not configured.

Command History

Release 9.1	Command was introduced.

Functional Notes

When enabled, the key will be stored in the generic routing encapsulation (GRE) header and the key present bit will be set. If tunnel keys are used, a matching key value must be defined on both endpoints of the tunnel or packets will be discarded.

Usage Examples

The following example sets the key on a tunnel interface to a value of **1234**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel key 1234**

tunnel protection ipsec profile *<name>*

Use the **tunnel protection ipsec profile** command to apply the IPsec profile to traffic egressing the tunnel. Use the **no** form of this command to remove the IPsec profile from the tunnel.

Syntax Description

<name>	Specifies the name of the IPsec profile to apply to the tunnel.

Default Values

By default, no IPsec profile is configured.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

The IPsec profile must be created before attempting to apply it to the tunnel. Refer to the command *ip crypto ipsec profile <name> on page 1351*. If the **tunnel protection ipsec profile** command is entered, and the profile has not been created, an error is returned.

If a crypto map is already configured on the tunnel interface, an error is returned if the **tunnel protection ipsec profile** command is entered.

Usage Examples

The following example applies the IPsec profile **PROFILE1** to the tunnel **1** interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel protection ipsec profile PROFILE1**

tunnel sequence-datagrams

Use the **tunnel sequence-datagrams** command to enable sequence number checking on incoming generic routing encapsulation (GRE) packets, to drop packets arriving out of order, and to include a sequence number in outgoing packets. Use the **no** form of this command to disable sequence number checking.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 9.1	Command was introduced.

Functional Notes

Both ends of the tunnel must have sequence numbering enabled. When both endpoints have sequence numbering enabled, a packet arriving with a sequence number less than the current expected value will be dropped. If the endpoints differ in their sequence numbering configuration, all packets will still flow without any sequence number verification. Be careful enabling sequence number verification on a tunnel. The tunnel can easily become out of sequence due to network conditions outside of the tunnel endpoints. It may be difficult to establish a successful traffic flow after an out of sequence condition occurs.

Usage Examples

The following example enables sequence number processing on the tunnel interface:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel sequence-datagrams**

Technology Review

When enabled, the next valid sequence number will be placed in the GRE header of each outgoing packet, and the sequence number present bit will be set.

tunnel source

Use the **tunnel source** command to specify the IP address or name of a physical interface to use as the source address for all packets transmitted on this interface. Use the **no** form of this command to clear the tunnel source address. Variations of this command include:

tunnel source <*ip address*>
tunnel source <*ip address*> <*interface*>

Syntax Description

<*ip address*>	Specifies the IP address in dotted decimal notation to use as the source address for all packets transmitted on this interface. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*interface*>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **tunnel source ?** for a complete list of valid interfaces.

Default Values

By default, a tunnel source is not defined.

Command History

Release 9.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.

Functional Notes

Until a tunnel interface has a source IP address defined and the physical interface used as the source is operational, the tunnel is not operational.

The tunnel source IP address will be the value put into the source field of the outer IP header after generic routing encapsulation (GRE) of the original packet.

Usage Examples

The following example sets the tunnel source IP address to **192.22.73.101**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel source 192.22.73.101**

The following example sets the tunnel source IP address to the address of the Ethernet interface labeled **0/1**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel source eth 0/1**

tunnel vrf <*name*>

Use the **tunnel vrf** command to specify the virtual routing and forwarding (VRF) to use in order to reach the tunnel source and the tunnel destination. Use the **no** form of this command to use the default VRF.

VRF on an AOS product allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF will affect the default unnamed VRF.

Syntax Description

<*name*>	Optional. Specifies the name of the VRF.

Default Values

By default, the default VRF is used.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the VRF instance to use to reach the tunnel source as VRF **RED**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#tunnel vrf RED**
(config-tunnel 1)**#tunnel source 10.10.10.254**
(config-tunnel 1)**#tunnel destination 10.10.10.1**

udp destination-port <*value*>

Use the **udp destination-port** command to specify a value for the virtual extensible local area network (VxLAN) user datagram protocol (UDP) destination port. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the UDP destination port for a VxLAN tunnel interface. Valid range is **1** to **65535**.

Default Values

By default, the VxLAN UDP destination port is set to **4789**.

Command History

Release R13.1.0	Command was introduced.

Usage Examples

The following example sets the VxLAN UDP destination port to 1525:

(config)**#interface tunnel 1 vxlan**
(config-tunnel 1)**#udp destination-port 1525**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the tunnel interface to the VRF instance named **RED**:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#vrf forwarding RED**

VLAN COMMAND SET

To activate the Virtual Local Area Network (VLAN) Configuration mode, enter the **vlan** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#vlan 1
(config-vlan 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

ip flow on page 3357
media ethernet on page 3358
name <name> on page 3359
state on page 3360

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables traffic monitoring on a virtual local area network (VLAN) interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface vlan 2**
(config-vlan 2)**#ip flow ingress myacl**

media ethernet

Use the **media ethernet** command to set the virtual local area network (VLAN) media type to Ethernet. The only media type currently supported is Ethernet. Use the **no** form of this command to reset to the default setting.

Syntax Description

No subcommands.

Default Values

By default, media is set to **Ethernet**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the media type to Ethernet for VLAN 2:

```
(config)#vlan 2
(config-vlan 2)#media ethernet
```


name <*name*>

Use the **name** command to assign a name to the virtual local area network (VLAN). Use the **no** form of this command to remove a name given to a VLAN.

Syntax Description

<*name*>	Assigns a name to the VLAN using **1** to **32** characters.

Default Values

By default, the name is set to VLANxxxx, where xxxx represents four numeric digits (including leading zeroes) equal to the VLAN ID number.

Command History

Release 5.1	Command was introduced.

Functional Notes

The name is limited to 32 characters and must be unique throughout.

Usage Examples

The following example sets the name of VLAN 2 to **Accounting**:

(config)**#vlan 2**
(config-vlan 2)**#name Accounting**

state

Use the **state** command to change the state of the virtual local area network (VLAN). Variations of this command include:

state active
state suspend

Syntax Description

active	Changes the VLAN state to active.
suspend	Changes the VLAN state to suspended.

Default Values

The default setting is **active** (once the VLAN has been created).

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the VLAN **state** to suspended:

(config)**#vlan 2**
(config-vlan 2)**#state suspend**

VLAN DATABASE COMMAND SET

To activate the Virtual Local Area Network (VLAN) Database Configuration mode, enter the **vlan database** command at the Enable security mode prompt. For example:

```
>enable
#configure terminal
(config)#vlan database
(vlan)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

abort on page 3362
apply on page 3363
reset on page 3364
show on page 3365
vlan <vlan id> on page 3366
vlan <vlan id> media ethernet on page 3367
vlan <vlan id> name <name> on page 3368
vlan <vlan id> state on page 3369

abort

Use the **abort** command to exit the virtual local area network (VLAN) database without saving any changes made.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this setting.

Command History

Release 5.1	Command was introduced.

Functional Notes

The **abort** command discards all configuration changes made since you entered the VLAN Database Configuration mode (or since the last time you issued the **apply** command). The system then exits out of this mode, returning to the enable (**#**) command prompt. Refer to the command *apply on page 3363* for more information.

Usage Examples

The following example exits the VLAN database without saving the changes made:

```
(config)#vlan database
(vlan)#abort
Discarding all changes and exiting.
#
```


apply

Use the **apply** command to apply changes without exiting the virtual local area network (VLAN) database.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this setting.

Command History

Release 5.1	Command was introduced.

Functional Notes

Applies changes to the VLAN database configuration in the running configuration.

Usage Examples

The following example applies changes made, remaining in the VLAN database:

```
(config)#vlan database
(vlan)#apply
Changes applied.
(vlan)#
```

reset

Use the **reset** command to discard all changes made and revert to the previous configuration. The prompt remains in the virtual local area network (VLAN) database.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this setting.

Command History

Release 5.1	Command was introduced.

Functional Notes

The **reset** command discards all changes to the VLAN configuration. The configuration remains the same as it was prior to entering the VLAN Database Configuration mode (or since the last time you issued the **apply** command). The VLAN database reverts to the same state it had upon entry. Refer to the command *apply on page 3363* for more information.

Usage Examples

The following example resets the unit to the previous configuration (i.e., the last configuration saved using the **apply** or the **exit** command):

```
(config)#vlan database
(vlan)#reset
VLAN configuration has been reset.
(vlan)#
```


show

Use the **show** command to display different aspects of the virtual local area network (VLAN) configuration. Variations of this command include:

show changes
show changes <*vlan id*>
show current
show current <*vlan id*>
show proposed
show proposed <*vlan id*>

Syntax Description

<*vlan id*>	Specifies a VLAN ID to display only information for a specific VLAN. Valid VLAN interface ID range is from **1** to **4094**.
changes	Displays the proposed changes to the VLAN configuration.
current	Displays the current VLAN configuration.
proposed	Displays the proposed VLAN database. The proposed version is not part of the running configuration until it is applied (using the **apply** command or the **exit** command).

Default Values

No default values are necessary for this setting.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example shows the proposed VLAN database configuration that will take effect if an **apply** or **exit** command is issued:

(config)**#vlan database**
(vlan)**#show proposed**

vlan <*vlan id*>

Use the **vlan** command to create a virtual local area network (VLAN) within the VLAN database. Use the **no** form of this command to delete a previously created VLAN from the database.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Range is **1** to **4094**.

Default Values

No default values are necessary for this setting.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example creates VLAN 2 only within the VLAN database. This VLAN is not added to the running configuration until an **exit** or **apply** command is issued:

```
(vlan)#vlan 2
VLAN 2 created.
Name = VLAN0002
(vlan)#
```

The following example removes VLAN 2 from the VLAN database. This VLAN is not removed from the running configuration until an **exit** or **apply** command is issued:

```
(config)#vlan database
(vlan)#no vlan 2
```

vlan <*vlan id*> media ethernet

Use the **vlan media ethernet** command to set the virtual local area network (VLAN) media type to Ethernet. Use the **no** form of this command to reset to the default setting.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Valid range is **1** to **4094**.

Default Values

By default, **vlan media** is set to **Ethernet**.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the media type of VLAN 2 to Ethernet:

(config)**#vlan database**
(vlan)**#vlan 2 media ethernet**

vlan <*vlan id*> **name** <*name*>

Use the **vlan name** command to assign a name to the virtual local area network (VLAN). Use the **no** form of this command to remove an assigned name.

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Valid range is **1** to **4094**.
<*name*>	Assigns a name to the VLAN using **1** to **32** characters.

Default Values

By default, the assigned name is VLANxxxx; where xxxx represents four numeric digits (including leading zeroes) equal to the VLAN ID number.

Command History

Release 5.1	Command was introduced.

Functional Notes

The name is limited to 32 characters and must be unique throughout the network.

Usage Examples

The following example sets the name of VLAN 2 to **Accounting**:

(config)**#vlan database**
(vlan)**#vlan 2 name Accounting**

vlan <*vlan id*> state

Use the **vlan state** command to change the state of the virtual local area network (VLAN). Use the **no** form of this command to return to the default setting. Variations of this command include:

vlan <*vlan id*> **state active**
vlan <*vlan id*> **state suspend**

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID. Valid VLAN ID range is **1** to **4094**.
active	Changes the VLAN state to active.
suspend	Changes the VLAN state to suspended.

Default Values

The default setting is **active** (once the VLAN has been created).

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the VLAN state to suspended:

(config)**#vlan database**
(vlan)**#vlan 2 state suspend**

VLAN INTERFACE COMMAND SET

To create a virtual local area network (VLAN) interface and/or activate the VLAN Interface Configuration mode, enter the **interface vlan** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface vlan 1
(config-interface-vlan 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

arp arpa on page 3372
awcp on page 3373
bandwidth <value> on page 3374
bridge-group <number> on page 3376
dynamic-dns on page 3377
ip commands begin on page 3379
ipv6 commands begin on page 3423
mac-address <mac address> on page 3460
max-reserved-bandwidth <value> on page 3461
media-gateway ip on page 3462
media-gateway ipv6 on page 3464
no shutdown track <name> on page 3466
ospfv3 commands begin on page 3467
packet-capture <name> on page 3480
qos-policy on page 3481
rtp quality-monitoring on page 3483
snmp trap on page 3484
snmp trap link-status on page 3485
traffic-shape rate <value> on page 3486

arp arpa

Use the **arp arpa** command to set ARPA as the standard Address Resolution Protocol (ARP) on this interface. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the ARP is set to **ARPA**.

Command History

Release 5.1	Command was introduced.
Release 6.1	Command was extended to include the NetVanta 2000 Series units.

Usage Examples

The following example enables standard ARP for the virtual local area network (VLAN) interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#arp arpa**

awcp

Use the **awcp** command to enable Adtran Wireless Control Protocol (AWCP) on this interface. The AWCP is an Adtran proprietary protocol used by an access controller (AC) to communicate with an access point (AP). Use the **no** form of this command to disable AWCP for this interface.

Syntax Description

No subcommands.

Default Values

By default, AWCP is enabled on the interface.

Command History

Release 15.1	Command was introduced.

Functional Notes

When the global-level command **dot11ap access-point-controller** (refer to *dot11ap access-point-control on page 1268* for more information) is enabled, the AWCP function can be disabled on a specific interface by using the **no** form of this command from the desired interface. When the global-level command **dot11ap access-point-controller** is disabled, it overrides the **awcp** command setting for the interface.

Usage Examples

The following example disables AWCP on virtual local area network (VLAN) 1:

```
(config)#interface vlan 1
(config-interface-vlan 1)#no awcp
```

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view the default values, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 3461*) to adjust the bandwidth appropriately for QoS configurations.

When configuring QoS for an Ethernet or VLAN interface, the interface **traffic-shape rate** command can be used to configure traffic shaping without applying a QoS map. If traffic shaping is applied to the same interface that will also have a QoS map applied to it, the amount of bandwidth available for the QoS policy is reduced to the value set with the **traffic-shape rate** command (*page 3486*). This value should be set to match the upload speed of the circuit. For example, under normal circumstances, an Ethernet interface can negotiate to 100 Mbps. However, the throughput of the upstream equipment is usually significantly less than the negotiated rate. The **traffic-shape rate** command is used to define the limit of when QoS policies containing the commands *bandwidth on page 4466* or *priority on page 4481* should be enforced according to the upload speed of the circuit. If the **bandwidth** <*value*> command is also entered on the same IP interface as the **traffic-shape rate** command, it will overwrite the value of the **traffic-shape rate** command for QoS purposes. It is not recommended to use the **bandwidth** <*value*> command for QoS. Instead, use the **max-reserved-bandwidth** command (*page 3461*) to adjust the bandwidth appropriately because the **traffic-shape rate** command is required for QoS to function properly on VLAN and Ethernet WAN IP interfaces.

Usage Examples

The following example sets bandwidth of the VLAN 1 interface to 10 Mbps:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#bandwidth 10000**

bridge-group *<number>*

Use the **bridge-group** command to assign an interface to the specified bridge group. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<number>	Specifies a bridge group number. Range is **1** to **255**.

Default Values

By default, there are no configured bridge groups.

Command History

Release 1.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (e.g., Ethernet to T1 bridge, Ethernet to Frame Relay subinterface).

Usage Examples

The following example assigns the virtual local area network (VLAN) interface to bridge group 17:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#bridge-group 17**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services Inc., (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#dynamic-dns dyndns-custom host user pass**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for IPv4 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Applies the named IPv4 ACL to the interface.
in	Enables access control on IPv4 packets received on the specified interface.
out	Enables access control on IPv4 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example configures the router to only allow IPv4 Telnet traffic (as defined in the user-configured **TelnetOnly** ACL) into the VLAN interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface vlan 1**
(config-vlan 1)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to an interface. IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an interface.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the Ethernet interface 0/1:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ip access-policy PRIVATE**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface (only one primary address is allowed). Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 /30**:

(config)**#interface vlan 1**
(config-vlan 1)**#ip address 192.22.72.101 /30 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii *<string>* **| hex** *<value>***] [client-id [***<interface>* **|** *<identifier>***]] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp client-id [*<interface>* **|** *<identifier>***] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp hostname *"<string>"* **[no-default-route | no-domain-name | no-nameservers] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track *<name>***] [***<administrative distance>***]**
ip address dhcp track *<name>* **[***<administrative distance>***]**

Syntax Description

<administrative distance>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii *<string>*	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex *<value>*	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<interface>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<identifier>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the *<identifier>* option.
hostname *<"string">*	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

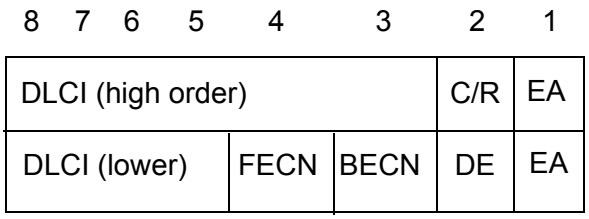
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *“<string>”* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#interface vlan 2**
(config-intf-vlan 2)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#interface vlan 2**
(config-intf-vlan 2)**#ip address dhcp hostname “adtran” no-default-route no-domain-name no-nameservers 5**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

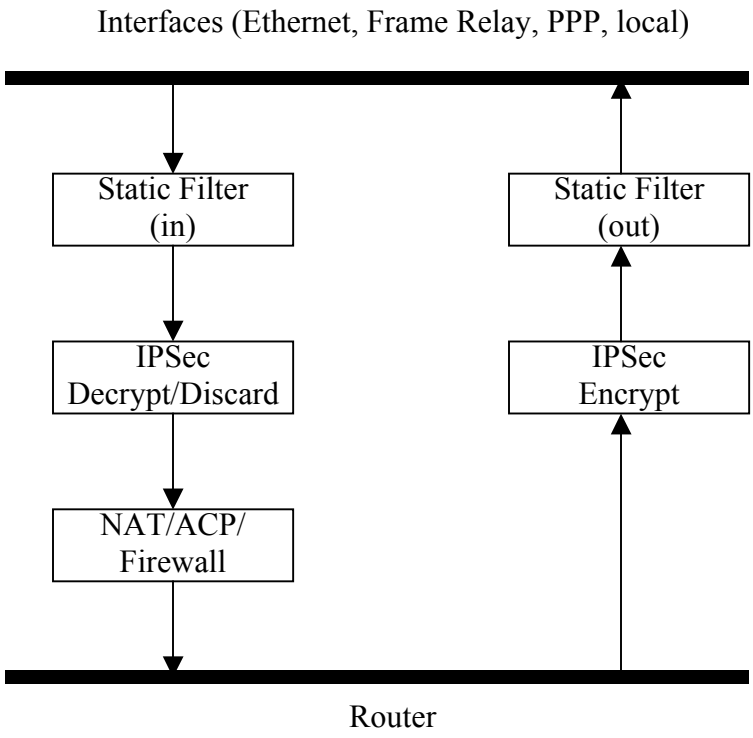
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Levell Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip crypto map MyMap**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).

Usage Examples

The following example releases the IPv4 DHCP address for the virtual local area network (VLAN) interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip dhcp release**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**)..

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#interface vlan 1**
(config-vlan 1)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **vlan 1**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 4 (IPv4) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries to be cleared from this IPv4 interface.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.4.0	Maximum number of stored entries was expanded to **500000** and RapidRoute is now enabled by default.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv4 interface:

(config)**#interface vlan 1**
(config-vlan 1)**#no ip ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper-address** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (**255.255.255.255**) or a subnet broadcast (for example, **192.33.4.251** for the **192.33.4.248 /30** subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.

Syntax Description

query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.
static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

ip igmp immediate-leave	No default
ip igmp last-member-query-interval	**1000** milliseconds
ip igmp querier-timeout	2x the **query-interval** value
ip igmp query-interval	**60** seconds
ip igmp query-max-response-time	**10** seconds
ip igmp static-group	No default
ip igmp version	Version **1**

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to **200** milliseconds:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface, and to place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 3402* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface vlan 1
(config-interface-vlan 1)#ip mcast-stub downstream
```


ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*ip address*> command to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 3399*, and *ip mcast-stub upstream on page 3402* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 3399* for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the interface:

((config)**#interface vlan 1**
(config-vlan 1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize Open Shortest Path First version 2 (OSPFv2) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **area** <*area id*>
ip ospf <*process id*> **authentication-key** <*password*>
ip ospf <*process id*> **cost** <*value*>
ip ospf <*process id*> **dead-interval** <*seconds*>
ip ospf <*process id*> **hello-interval** <*seconds*>
ip ospf <*process id*> **message-digest-key [1 | 2] md5** <*key*>
ip ospf <*process id*> **priority** <*value*>
ip ospf <*process id*> **retransmit-interval** <*seconds*>
ip ospf <*process id*> **shutdown**
ip ospf <*process id*> **transmit-delay** <*seconds*>

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
area <*area id*>	Specifies the ID of the area to which this interface is assigned for the specified OSPFv2 process. Valid range is **0** to **4294967295**.
authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.

shutdown	Disables the OSPFv2 process on the interface. When this keyword is used, the OSPFv2 settings remain in place, but logically it appears to the interface as though the process has been removed from the configuration. This parameter can be useful in troubleshooting.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*>, **area** <*area id*>, and **shutdown** parameters.

Usage Examples

The following example sets the maximum number of seconds allowed between hello packets to **25000**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip ospf 1 dead-interval 25000**

ip ospf <*process id*> authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **authentication**
ip ospf <*process id*> **authentication message-digest**
ip ospf <*process id*> **authentication null**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
message-digest	Optional. Selects message digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Usage Examples

The following example specifies that no authentication will be used on the virtual local area network (VLAN) interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip ospf 1 authentication null**

ip ospf <*process id*> network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf <*process id*> **network broadcast**
ip ospf <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv2 routing process this interface is to join. The process ID is locally significant to the device, and must be unique among all OSPFv2 processes on the device. Valid range is **1** to **65535**.
broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to **point-to-point**.

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command was expanded to include the <*process id*> parameter.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip ospf 1 network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the virtual local area network (VLAN) 1 interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the virtual local area network (VLAN) 1 interface every **3600** seconds:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to **300** seconds:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation delay to **300** milliseconds:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip pim-sparse propagation-delay 300**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all proxy ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the virtual local area network (VLAN) interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only RIP version 1 packets received on the interface.
2	Accepts only RIP version 2 packets received on the interface.

Default Values

By default, all interfaces implement RIP **version 1** (the default value for the version command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual local area network (VLAN) interface to accept only RIP **version 2** packets:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP **version 1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual local area network (VLAN) interface to transmit only RIP **version 2** packets:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable Internet Protocol version 4 (IPv4) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.

Functional Notes

Fast switching allows an IPv4 interface to provide optimum performance when processing IPv4 traffic.

Usage Examples

The following example enables IPv4 fast switching on the VLAN interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ip route-cache**

ip route-cache express

Use the **ip route-cache express** command to enable Layer 3 switching on the virtual local area network (VLAN) interface. Use the **no** form of this command to disable Layer 3 switching on the interface.

Syntax Description

No subcommands.

Default Values

Layer 3 switching is disabled by default, except on the NetVanta 1544. Layer 3 switching is enabled by default on the NetVanta 1544.

Functional Notes

Layer 3 switching cannot be disabled on the NetVanta 1544.

Enabling or disabling Layer 3 switching on the VLAN interfaces overrides the global Layer 3 switching configuration.

For more information about Layer 3 switching, refer to the *Layer 3 Switching in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example enables Layer 3 switching on VLAN **200**:

```
(config)#interface vlan 200
(config-intf-vlan 200)#ip route-cache express
```

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface that contains the IP address to use as the source address for all packets transmitted on this interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **ip unnumbered ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interfaces.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Frame Relay Subinterface Configuration mode configures the Frame Relay subinterface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the virtual local area network (VLAN) interface (labeled **vlan 1**) to use the IP address assigned to the Ethernet interface (**eth 0/1**):

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip unnumbered eth 0/1**

ip urlfilter <*name*>

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<*name*>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** <*name*> **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the VLAN interface and matches the URL filter named **MyFilter**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on an interface. Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the interface.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the interface to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the interface.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an interface when other unicast IPv6 addresses are not needed on the interface. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the interface.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the interface:

```
(config)#interface vlan 1
(config-vlan 1)#ipv6
```

ipv6 access-group *<ipv6 acl name>*

Use the **ipv6 access-group** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to be used for IPv6 packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ipv6 access-group <*ipv6 acl name*> **in**
ipv6 access-group <*ipv6 acl name*> **out**

Syntax Description

<ipv6 acl name>	Applies the named IPv6 ACL to the interface.
in	Enables access control on IPv6 packets received on the specified interface.
out	Enables access control on IPv6 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 18.1	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Only one IPv6 ACL can be applied in each traffic direction.

Unlike in IPv4, IPv6 traffic filters include an implicit **permit** for neighbor solicitation and advertisement packets in an ACL before the traditional implicit **deny** at the end of the ACL. This prevents blocking of address resolution and unreachability detection, although this can be overridden by entering explicit **deny** commands in the IPv6 ACL.

Usage Examples

The following example applies the IPv6 ACL **Privatev6** to incoming IPv6 traffic on the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 access-group Privatev6 in**

ipv6 access-policy *<ipv6 acp name>*

Use the **ipv6 access-policy** command to assign a specified Internet Protocol version 6 (IPv6) access control policy (ACP) to an interface. IPv6 ACPs are applied to IPv6 traffic entering an interface. Use the **no** form of this command to remove an ACP association.

Syntax Description

<ipv6 acp name>	Identifies the configured IPv6 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv6 ACPs associated with an interface.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example applies the IPv6 ACP **PRIVATEv6** to the interface:

Enable the AOS security features:
(config)**#ipv6 firewall**

Associate the ACP with the VLAN interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 access-policy PRIVATEv6**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3428*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

Command History

Release 18.1	Command was introduced.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the interface using the command *ipv6 address <ipv6 link-local address> link-local on page 3428*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the interface and enables IPv6 processing on the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address <*ipv6 link-local address*> link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

Syntax Description

<*ipv6 link-local address*>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the interface.

Default Values

By default, no IPv6 address is configured for the interface and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

A single link-local address can be manually configured on an interface. The lower 64 bits of the specified address become the Interface ID for the interface, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the interface and can be derived from the interface's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the interface.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

Usage Examples

The following example manually creates a link-local IPv6 address on the interface and enables IPv6 processing:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 address autoconfig

Use the **ipv6 address autoconfig** command to enable Internet Protocol version 6 (IPv6) processing on the interface, create a local-link IPv6 address for the interface, and allow the interface to automatically configure itself based on advertisements from other routers on the link. Use the **no** form of this command to remove all autoconfigured addresses, prefixes, and any resulting routes from the interface and also causes the interface to cease processing received router advertisements (RAs).Variations of this command include:

ipv6 address autoconfig
ipv6 address autoconfig default
ipv6 address autoconfig default metric <*value*>

Syntax Description

default	Optional. Specifies that the interface maintain a list of advertising routers that are willing to be IPv6 default routers.
metric <*value*>	Optional. Specifies the administrative distance for a default router maintained in the default router list. Range is **1** to **255**. Routes with lower administrative distance are favored.

Default Values

By default, no IPv6 addresses are configured for the interface and IPv6 processing is not enabled. When an IPv6 address is configured automatically, the administrative distance for default routers is **2** by default.

Command History

Release 18.1	Command was introduced.

Functional Notes

When autoconfiguration is enabled, the interface listens for RA messages that tell the interface how it should be configured. The interface then creates addresses for advertised 64-bit prefixes with the A flag in the IPv6 address set using stateless address autoconfiguration (SLAAC). The addresses use the EUI-64 interface ID in the lower 64 bits of the address. A route type of *Connected* is added to the route table if the L flag on the prefix advertisement (on-link flag) is also set.

Usage Examples

The following example enables IPv6 processing on the interface, creates a link-local IPv6 address for the interface, and allows the interface to automatically configure itself for IPv6:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 address autoconfig**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname <*partial fqdn*>
ipv6 address dhcp hostname fqdn <*fqdn*>
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 3423*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 address 2001:DB8:1::1/64**
(config-vlan 1)**#ipv6 address dhcp fqdn client@company.com**

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*

Use the **ipv6 address named-prefix** command to create an Internet Protocol version 6 (IPv6) address for the interface using the values in a named prefix. Use the **no** form of this command to remove the address from the interface. Variations of this command include:

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*
ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>* **eui-64**

Syntax Description

<prefix name>	Specifies the named prefix to use to create the address.
<ipv6 address/prefix-length>	Specifies the address portion appended to the named prefix to create a 128-bit host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
eui-64	Optional. Indicates that the interface ID is to be placed in the lower 64 bits of the address.

Default Values

By default, no IPv6 addresses are specified on the interface.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example creates an IPv6 address on the interface using the named prefix **PREFIX1**:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 address named-prefix PREFIX1 2001:1:0:/48**

ipv6 crypto map *<name>*

Use the **ipv6 crypto map** command to associate Internet Protocol version 6 (IPv6) crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

Syntax Description

<name>	Specifies the IPv6 crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Only one IPv6 crypto map can be specified per interface, and the crypto map is applied within the virtual routing and forwarding (VRF) instance to which the interface belongs. To apply the IPv6 crypto map, the interface must have IPv6 enabled. In addition, the interface must have an IPv6 address of appropriate scope to allow connectivity to peer's addresses as specified in the crypto map's entries.

Usage Examples

The following example applies all IPv6 crypto maps with the name **MyMap** to the interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ipv6**
(config-interface-vlan 1)**#ipv6 crypto map MyMap**

ipv6 dhcp client information refresh minimum <*seconds*>

Use the **ipv6 dhcp client information refresh minimum** command to specify the minimum value the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the interface accepts as its information refresh timer. Use the **no** version of this command to return to the default setting.

Syntax Description

<*seconds*>	Specifies the refresh timer in seconds. Valid range is **600** to **3600** seconds.

Default Values

By default, the DHCPv6 client refresh timer is set to **600** seconds.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example specifies the DHCPv6 client refresh timer for the interface is **800** seconds:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 dhcp client information refresh minimum 800**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 dhcp client pd PREFIX1**

ipv6 dhcp relay destination *<ipv6 address>*

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the interface. Variations of this command include:

ipv6 dhcp relay destination *<ipv6 address>*
ipv6 dhcp relay destination *<ipv6 address> <interface>*

Syntax Description

<ipv6 address>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** *<ipv6 address>* **?** to display a list of valid interfaces.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R13.7.0	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

To configure an interface to function as a DHCPv6 relay agent, you must first enable IPv6 on the interface using the command *ipv6 on page 3423*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ipv6**
(config-interface vlan 1)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped mulitcast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the interface and specify that the interface is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the interface, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the interface. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this interface. All DHCPV^ requests received on this interface are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Enabling the interface as a DHCPv6 server using this command places the interface into DHCPv6 server mode. DHCPv6 modes (server or relay) are mutually exclusive at the interface. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the interface as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 address 2001:DB8:1::1/64**
(config-vlan 1)**#ipv6 dhcp server POOL1**

ipv6 ffe

Use the **ipv6 ffe** command to enable the RapidRoute fast forwarding engine (FFE) on this Internet Protocol version 6 (IPv6) interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 ffe
ipv6 ffe max-entries <*value*>

> NOTE *Issuing this command will cause all RapidRoute entries to be cleared from this IPv6 interface.*

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **500000**.

Default Values

By default, the RapidRoute Engine is enabled on IPv6-enabled interfaces (using the command *ipv6 on page 2231*). The default number of **max-entries** is **4096**.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example disables RapidRoute on the IPv6 interface:

(config)**#interface vlan 1**
(config-vlan 1)**#no ipv6 ffe**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the interface in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the interface.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the interface in host mode:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 mode host unicast**

ipv6 mtu *<size>*

Use the **ipv6 mtu** command to specify the maximum transmission unit (MTU) for Internet Protocol version 6 (IPv6) packets on the interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Specifies the MTU value. Valid range is **1280** to **1500** bytes.

Default Values

By default, the MTU of the interface is set to **1280** bytes.

Command History

Release 18.1	Command was introduced.

Functional Notes

In IPv6, the minimum MTU is 1280 octets. Any link that has an MTU less than 1280 octets must use link fragmentation and reassembly that is transparent to IPv6 (for example, the Fragmentation Header). Sources in the IPv6 network are expected to perform path maximum transmission unit (PMTU) discovery to send packets larger than 1280 octets. PMTU works in the following manner: First, the sending node assumes the link MTU of the interface from which the traffic is being forwarded and then sends the IPv6 packet at the link MTU size. If a router on the path is unable to forward the packet, it sends an ICMP *Packet Too Big* message back to the sending node containing the link MTU of the link on which the packet forwarding failed. The sending node then rests the PMTU to the value of the MTU field in the Internet Control Message Protocol version 6 (ICMPv6) *Packet Too Big* message, and the packet is resent.

The MTU for IPv6 packets can be set on a per-interface basis. There are two methods for setting MTUs for interfaces if required: one for Layer 3 interfaces, and one for the underlying Layer 1 and Layer 2 interfaces. For all interface types, use the **ipv6 mtu** *<size>* command to specify the IPv6 MTU in bytes from the interface's configuration mode. The minimum MTU setting for IPv6 is **1280** bytes, and the maximum is **1500** bytes. The IPv6 MTU value is independent of the IPv4 MTU setting (set with the command *ip mtu <size> on page 3403*).

When the interface is forwarding the IPv6 packet as a router, if the packet size exceeds the IPv6 MTU of the egress interface, the packet is dropped and ICMPv6 *Packet Too Big* message is sent to the source. When originating an IPv6 packet from the local IPv6 stack, and the packet is larger than the IPv6 MTU of the egress interface, the packet is fragmented and sent.

Usage Examples

The following example specifies the IPv6 MTU value for the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 mtu 1350**

ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** command to specify that the Advertisement Interval Option is sent in Internet Protocol version 6 (IPv6) router advertisement (RA) messages from the router. This command is effectual only when the interface is in router mode. Use the **no** form of this command to return to the default interval.

Syntax Description

No subcommands.

Default Values

By default, Advertisement Interval Options are not sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

Sending the Advertisement Interval Option should be enabled when the router is functioning in a mobile IP environment to aid movement detection by mobile nodes. This option contains the current value of the maximum router advertisement interval configured using the command *ipv6 nd ra interval on page 3454*.

Usage Examples

The following example specifies that the interface include Advertisement Interval Options in RA messages sent from the router:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd advertisement-interval**

ipv6 nd cache max-incomplete <*number*>

Use the **ipv6 nd cache max-incomplete** command to specify the maximum number of incomplete entries the Neighbor Discovery (ND) cache retains. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of incomplete ND entries to retain in the cache. Valid range is **1** to **321**.

Default Values

By default, the incomplete ND entries can take at maximum one-third of the possible ND cache entries (varies by product).

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example specifies that the interface stores **150** incomplete entries in the ND cache:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd cache max-incomplete 150**

ipv6 nd dad attempts <*number*>

Use the **ipv6 nd dad attempts** command to specify the number of neighbor solicitation (NS) messages sent by the interface when performing Internet Protocol version 6 (IPv6) duplicate address detection (DAD). This command is effectual when the interface is in either host or router mode. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of NS messages that will be sent. Range is **0** to **10** messages. A value of **0** disables DAD on the interface.

Default Values

By default, the interface sends **1** NS message.

Command History

Release 18.1	Command was introduced.

Functional Notes

DAD is used by devices to determine if IPv6 addresses are unique before they are applied to interfaces. DAD is used in NS messages to detect duplicate unicast addresses. The Target Address fields in the NS messages are set to the IPv6 address for which duplication is being detected. Destination IPv6 addresses for DAD in NS messages are the solicited-node multicast version of the address being tested. Source IPv6 addresses for DAD are set to the IPv6 unspecified address (::). Once the IPv6 address is determined by DAD to be unique, it can be applied to the IPv6 interface on the node.

DAD in AOS is performed when an interface transitions state from DOWN to UP or when manually configuring an address. When performing DAD because of an interface transition, DAD will happen immediately after the interface transition and again 40 seconds later to cooperate with the port being connected to an Ethernet switch.

Usage Examples

The following example specifies that **3** NS messages are sent by the interface when performing DAD:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd dad attempts 3**

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command to specify the M flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. The M flag instructs hosts receiving the RA that they can use stateful Dynamic Host Configuration Protocol version 6 (DHCPv6) to configure addresses and nonaddress information. Use the **no** form of this command to disable the setting of the M flag.

Syntax Description

No subcommands.

Default Values

By default, the M flag is not set in RAs.

Command History

Release 18.1	Command was introduced.

Functional Notes

If you specify that the M flag is set in RA messages, you do not need to set the 0 flag (it becomes redundant).

Usage Examples

The following example sets the M flag for RA messages sent by the interface:

```
(config)#interface vlan 1
(config-vlan 1)#ipv6 nd managed-config-flag
```

ipv6 nd ns-interval *<value>*

Use the **ipv6 nd ns-interval** command to specify the interval between transmission of certain Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages and to control what ND value is advertised in router advertisement (RA) messages. This command is effectual whether the interface is in host or router mode. Use the **no** form of this command to return the interval to the default value.

Syntax Description

<value>	Specifies the time (in milliseconds) between neighbor message transmissions. Valid range is **1000** to **3600000** ms.

Default Values

By default, the interval is set to **1000** ms for internal use by the router and **0** (unspecified) is sent in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command controls the spacing of neighbor solicitation (NS) messages for functions such as address resolution, reachability detection, and duplicate address detection (DAD). For DAD it also serves as the amount of time after the last transmission before the detection phase of autoconfiguration terminates. In addition, the command controls the interval between unsolicited neighbor advertisement (NA) messages.

Usage Examples

The following example changes the interval between RA messages sent from the interface to **2000** ms:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd ns-interval 2000**

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command to specify the O flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. When the O flag is set, hosts receiving the RA messages are instructed that they may use stateless Dynamic Host Configuration Protocol version 6 (DHCPv6) to receive information that is not IPv6 addressing information, and to use some other method (whether through manual configuration, stateless address autoconfiguration (SLAAC), etc.) for addressing information. Use the **no** form of this command to disable the O flag setting.

Syntax Description

No subcommands.

Default Values

By default, the O flag is not set in RA messages.

Command History

Release 18.1	Command was introduced.

Functional Notes

If the M flag is set for RA messages, you do not need to set the O flag.

Usage Examples

The following example sets the O flag in RA messages from the interface:

```
(config)#interface vlan 1
(config-vlan 1)#ipv6 nd other-config-flag
```

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the interface. Use the **no** form of this command to remove the specified prefix configuration from the interface. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the interface is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the interface. Prefixes for IPv6 addresses configured on a router interface are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the interface.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the interface's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ipv6 nd purge-timer <*value*>

Use the **ipv6 nd purge-timer** command to specify the maximum amount of time an unused Internet Protocol version 6 (IPv6) neighbor entry remains in the neighbor cache. This command applies to interfaces in either host or router mode. Use the **no** form of this command to return the purging interval to the default value.

Syntax Description

<*value*>	Specifies the neighbor cache entry storage time in minutes. Valid range is **10** to **1440** minutes.

Default Values

By default, idle (STALE) neighbor cache entries are cleared after **1440** minutes (24 hours).

Command History

Release 18.1	Command was introduced.

Functional Notes

This command applies to interfaces in either router or host mode. A neighbor entry is typically purged when neighbor unreachability detection (NUD) is invoked and the neighbor is determined to no longer be reachable. However, NUD is not performed on idle (STALE) neighbor entries, so this command provides a method for purging unused entries after a specified amount of time.

Usage Examples

The following example specifies that idle neighbor entries in the neighbor cache are removed after **800** minutes:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd purge-timer 800**

ipv6 nd ra interval

Use the **ipv6 nd ra interval** command to specify the interval between transmission of Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the interface is in router mode. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 nd ra interval *<max time>*
ipv6 nd ra interval *<max time> <min time>*
ipv6 nd ra interval msec *<max time>*
ipv6 nd ra interval msec *<max time> <min time>*

Syntax Description

<max time>	Specifies the maximum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **4** to **1800** seconds and **70** to **1800000** ms.
<min time>	Optional. Specifies the minimum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **3** seconds to 75 percent of the configured maximum time value in seconds, or **30** ms to 75 percent of the configured maximum time value in ms.
msec	Optional. Specifies that the time values are in milliseconds.

Default Values

By default, the interval is set in seconds and has a maximum interval time of **200** seconds and a minimum interval time of 75 percent of the maximum seconds value, but not less than **3** seconds.

Command History

Release 18.1	Command was introduced.

Functional Notes

If this router is used as a default router, the interval between RA messages should not be set to a larger value than the RA lifetime set by the command *ipv6 nd ra lifetime <value> on page 3455*, which has a default value of **1800** seconds.

Usage Examples

The following example specifies that the maximum interval in seconds between RA message transmissions is **300**:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd ra interval 300**

ipv6 nd ra lifetime <*value*>

Use the **ipv6 nd ra lifetime** command to specify the router lifetime advertised in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is effectual when the interface is in router mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

ipv6 nd ra lifetime <*value*>
ipv6 nd ra lifetime default-route

Syntax Description

<*value*>	Specifies the router lifetime in seconds. Range is **0** to **9000** seconds. A value of **0** indicates this is not a default router. A value other than 0 indicates to other nodes that this router can be used as a default router.
default-route	Specifies the RA lifetime is **0** if no default route exists on any IPv6 interface.

Default Values

By default, the router lifetime is set to **1800** seconds.

Command History

Release 18.1	Command was introduced.
Release R11.5.0	Command was expanded to include the **default-route** parameter.

Functional Notes

A value other than **0** for a router lifetime should be larger than the router advertisement interval specified in the command *ipv6 nd ra interval on page 3454*.

Usage Examples

In the following example, the router lifetime advertised in RA messages is **3000** seconds:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd ra lifetime 3000**

ipv6 nd ra reachable-time <*value*>

Use the **ipv6 nd ra reachable-time** command to specify the value advertised for reachable time in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command also specifies the internal base reachable time used by the router. This command is effectual for interfaces in either host or router mode. Use the **no** form of this command to return the reachability value to the default setting.

Syntax Description

<*value*>	Specifies the reachability time in milliseconds. Range is **0** to **3600000** ms. A value of **0** indicates the reachable time is unspecified.

Default Values

By default, the router advertises a reachability time of **0** ms and uses an internal value of **30000** ms.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command is effectual for interfaces in either router or host mode. For hosts, this value sets the internal reachable time used by the host if no RAs are received specifying a different value. For routers, the value indicates the amount of time a device is considered reachable after having received a reachability confirmation in neighbor unreachabililty detection (NUD).

Usage Examples

The following example specifies that a reachability time of **50000** ms is advertised in RA messages:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd ra reachable-time 50000**

ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command to specify whether Internet Protocol version 6 (IPv6) router advertisement (RA) messages will be suppressed. This command only applies to interfaces in router mode. Use the **no** form of this command to begin sending RA messages.

Syntax Description

No subcommands.

Default Values

By default, RA messages are not suppressed. When IPv6 routing is not enabled on the router, or when implemented in a host-only mode, the default setting is to suppress advertisements on all interface types.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example suppresses RA messages on the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd ra suppress**

ipv6 nd router-preference

Use the **ipv6 nd router-preference** command to specify the default router preference value set in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. Setting this preference helps the receivers of RA messages to determine the preference of one router over another as a default router in environments with multiple routers. Use the **no** form of this command to return the preference to the default setting. Variations of this command include:

ipv6 nd router-preference high
ipv6 nd router-preference low
ipv6 nd router-preference medium

Syntax Description

high	Specifies the preference value is high.
low	Specifies the preference value is low.
medium	Specifies the preference value is medium.

Default Values

By default, the router preference is set to medium.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies that the advertised default router preference is high:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 nd router-preference high**

ipv6 route-cache

Use the **ipv6 route-cache** command to enable Internet Protocol version 6 (IPv6) fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 18.2	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.

Functional Notes

Fast switching allows an IPv6 interface to provide optimum performance when processing IPv6 traffic.

Usage Examples

The following example enables IPv6 fast switching on the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#ipv6 route-cache**

mac-address *<mac address>*

Use the **mac-address** command to specify the medium access control (MAC) address of the virtual local area network (VLAN) interface. Only the last three values of the MAC address can be modified. The first three values contain the Adtran reserved number (00:0A:C8) by default. Use the **no** form of this command to return to the default MAC address programmed by Adtran.

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

A unique default MAC address is programmed in each unit shipped by Adtran.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures a MAC address of **00:0A:C8:5F:00:D2**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#mac-address 00:0A:C8:5F:00:D2**

max-reserved-bandwidth <*value*>

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<*value*>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies **85** percent of the bandwidth on the virtual local area network (VLAN) 1 interface be available for use in user-defined queues:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#max-reserved-bandwidth 85**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip primary vrrp <*number*>
media-gateway ip primary vrrpv3 <*number*>
media-gateway ip secondary <*ipv4 address*>
media-gateway ip secondary vrrp <*number*>
media-gateway ip secondary vrrp <*number*> <*ipv4 address*>
media-gateway ip secondary vrrpv3 <*number*>
media-gateway ip secondary vrrpv3 <*number*> <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vrrp <*number*>	Specifies that the IPv4 address of the Virtual Router Redundancy Protocol version 2 (VRRP) router group's virtual router ID (VRID) is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
vrrpv3 <*number*>	Specifies that the IPv4 address of the VRRP version 3 (VRRPv3) VRID is used as the media gateway address on the interface. Valid VRID range is **1** to **255**.
<*ipv4 address*>	Optional. Specifies a secondary IPv4 address of the VRRP or VRRPv3 VRID is used as the media gateway address on the interface. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A4.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.
Release R12.2.0	Command was expanded to include the **vrrp** and **vrrpv3** parameters.

Functional Notes

To use VRRP or VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRP or VRRPv3.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface vlan 1**
(config-vlan 1)**#media-gateway ip primary**

media-gateway ipv6

Use the **media-gateway ipv6** command to associate an Internet Protocol version 6 (IPv6) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv6 address associated with it. However, some interfaces allow dynamic configuration of IPv6 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ipv6
media-gateway ipv6 <*ipv6 address*>
media-gateway ipv6 loopback <*interface id*>
media-gateway ipv6 vrrpv3 <*number*>
media-gateway ipv6 vrrpv3 <*number*> <*ipv6 address*>

Syntax Description

<*ipv6 address*>	Specifies an IPv6 address to use for the media gateway. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
loopback <*interface id*>	Specifies an IPv6 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv6 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
vrrpv3 <*number*>	Specifies that all the secondary IPv6 addresses of the Virtual Routing Redundancy Protocol version 3 (VRRPv3) virtual router ID (VRID) are used as media gateway addresses on the interface. Valid VRID range is **1** to **255**.
<*ipv6 address*>	Optional. Specifies a single IPv6 address of the VRRPv3 VRID is used as the media gateway address on the interface. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

Default Values

By default, **media-gateway ipv6** is disabled.

Command History

Release R10.8.0	Command was introduced.
Release R12.2.0	Command was expanded to include the **vrrpv3** parameters.

Functional Notes

To use VRRPv3 addresses as the media gateway on the interface, you must first have configured VRRPv3.

Usage Examples

The following example configures the unit to use the IPv6 address for RTP traffic:

(config)**#interface vlan 1**
(config-vlan 1)**#media-gateway ipv6**

no shutdown track *<name>*

Use the **no shutdown track** command to restore the VLAN interface when the specified track passes. For more information about tracks, refer to *track <name> on page 1886* and the *Network Monitor Track Command Set on page 4098*.

Syntax Description

<name>	Specifies the name of the track to associate with the activation of the interface.

Default Values

By default, this command is not configured.

Command History

Release 17.5	Command was introduced.
Release R11.5.0	Command was expanded to include the virtual local area network (VLAN) interfaces.

Usage Examples

The following example enables the interface based on the specified track:

(config)**#interface vlan 1**
(config-vlan 1)**#no shutdown track work-hours**

ospfv3 <*process id*> **area** <*area id*>

Use the **ospfv3 area** command to add an interface to an Open Shortest Path First version 3 (OSPFv3) process, and to configure the OSPFv3 process on the interface. This command places the interface in the specified area for the specified Internet Protocol version 6 (IPv6) OSPFv3 address family, and optionally defines the instance ID that is used to represent this OSPFv3 process in messages on the interface's link. Use the **no** form of this command to remove the OSPFv3 process from the interface. Variations of this command include:

ospfv3 <*process id*> **area** <*area id*> **ipv6**
ospfv3 <*process id*> **area** <*area id*> **ipv6 instance** <*instance id*>

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join, for the specified address family. The process ID is locally significant to the device, and must be unique among all OSPFv3 processes on the device. Valid range is **1** to **65535**.
<*area id*>	Specifies the ID of the area to which this interface is assigned for the given OSPFv3 process. Valid range is **0** to **4294967295**.
ipv6	Identifies the OSPFv3 address family as IPv6.
instance <*instance id*>	Optional. Specifies the value to use in the instance ID field of messages sent or received by this OSPFv3 process on the interface's link. Valid range is **0** to **31**.

Default Values

By default, an OSPFv3 process is not configured on an interface. By default, process IDs, area IDs, and instance IDs are not defined.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

When using this command to enable an OSPFv3 process on an interface, keep the following rules in mind:

- The interface must have the address family enabled on the interface. If the address family is not enabled on the interface, the command is rejected and an error is displayed.
- Only interfaces on the default virtual routing and forwarding (VRF) instance support this command. Interfaces on a nondefault VRF will display an error when you attempt to configure OSPFv3 settings.
- The interface and the specified OSPFv3 process (if defined in the global configuration) must be in the same VRF or the command will fail.
- The address family must match that specified for the OSPFv3 process if the process has been defined in the global configuration or the command will fail.
- If the OSPFv3 process identified by the process ID does not exist in the global configuration, it is automatically created, along with the specified address family, and it is assigned to the VRF of which the interface is a member.

- If the specified OSPFv3 process is already at its maximum limit of processes or address families, the command fails.
- If the specified OSPFv3 process already exists in the global configuration, but its configuration does not include an address family, the specified address family is added to the OSPFv3 router configuration.
- A given OSPFv3 process can only have one address family.
- Multiple OSPFv3 instances per address family, per VRF, can be created and can be assigned to a given interface.
- If the interface's VRF changes, all OSPFv3 assignments are removed.
- To change an OSPFv3 process's VRF, the process must first be removed and then recreated. Removing the process removes all OSPFv3 assignments for that process form all interfaces.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To add an interface to the OSPFv3 process **5**, in area **10**, with an instance ID of **10**, enter the command as follows:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 5 area 10 ipv6 instance 10**

ospfv3 authentication

Use the **ospfv3 authentication** command to authenticate an interface that is performing Internet Protocol version 6 (IPv6) Open Shortest Path First version 3 (OSPFv3) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ospfv3 authentication ipsec spi <*spi*> **md5** <*key*>
ospfv3 authentication ipsec spi <*spi*> **sha1** <*key*>
ospfv3 authentication null

Syntax Description

ipsec	Specifies that IP security (IPsec) authentication is used.
spi <*spi*>	Specifies the security parameter index (SPI). Valid range is **256** to **4294967295**.
md5 <*key*>	Specifies that MD5 authentication is used. Keys are specified in 32 hexadecimal characters.
sha1 <*key*>	Specifies that SHA-1 authentication is used. Keys are specified in 40 hexadecimal characters.
null	Specifies that no OSPFv3 authentication is used.

Default Values

By default, this is set to **null** (meaning no authentication is used).

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example specifies that no OSPFv3 authentication will be used on the interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 authentication null**

ospfv3 *<process id>* **cost** *<cost>*

Use the **ospfv3 cost** command to specify a value that represents the cost of sending an Open Shortest Path First version 3 (OSPFv3) packet over the interface. Use the **no** form of this command to return the cost to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
cost *<cost>*	Specifies the OSPFv3 cost of the interface. This value overrides any automatically computed cost value (default value). Valid range is **1** to **65535**.

Default Values

By default, the OSPFv3 cost of the interface is automatically computed. The automatic cost computation is the reference bandwidth divided by the interface bandwidth. The reference bandwidth is set by the command *auto-cost reference-bandwidth <value> on page 4150*, and defaults to **100** Mbps.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the OSPFv3 cost of the interface as **10**:

```
(config)#interface vlan 1
(config-interface-vlan 1)#ospfv3 5 cost 10
```

ospfv3 <*process id*> dead-interval <*value*>

Use the **ospfv3 dead-interval** command to specify the maximum interval allowed between Open Shortest Path First version 3 (OSPFv3) Hello packets on the interface. If the maximum interval is exceeded, neighboring devices will assume that the device is down. This value must be the same across all interfaces on a link. Use the **no** form of this command to return the dead interval to the default value.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
dead-interval <*value*>	Specifies the maximum number of seconds allowed between OSPFv3 Hello packets. It is recommended that this value be **4** times the Hello packet interval (set with the command *ospfv3 <process id> hello-interval <value> on page 3474*). Valid range is **1** to **65535** seconds.

Default Values

By default, the maximum interval allowed between OSPFv3 Hello packets is set to **40** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

To specify the dead interval between OSPFv3 Hello packets on the interface, enter the command as follows:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 5 dead-interval 100**

ospfv3 encryption

Use the **ospfv3 encryption** command to specify a symmetrical, bidirectional Open Shortest Path First version 3 (OSPFv3) security association (SA) that uses encapsulating security payload (ESP) for encryption and authentication of all OSPFv3 messages that are sent or received on the interface. This command allows you to specify OSPFv3 security at the interface level. Use the **no** form of this command to remove IP security (IPsec) protection of OSPFv3 messages on the interface. Variations of this command include:

ospfv3 encryption ipsec spi <*spi*> **esp** <*encryption type*> <*encryption key*> <*authentication type*> <*authentication key*>
ospfv3 encryption ipsec spi <*spi*> **esp null** <*authentication type*> <*authentication key*>
ospfv3 encryption null

Syntax Description

ipsec	Specifies that IPsec encryption is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by any other IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
esp	Specifies that ESP is used.
null	Specifies that OSPFv3 messages on this interface are not encrypted when used in the **ospfv3 encryption null** format (even when encryption is specified by the OSPFv3 area configuration). When used in the **ospfv3 encryption ipsec spi** <*spi*> **esp null** format, **null** indicates that messages on the interface will not be encrypted, but will be authenticated.
<*encryption type*>	Specifies the type of algorithm used to encrypt OSPFv3 messages. Valid values for encryption are: **3des** uses triple data encryption standard (DES). **aes-cbc** uses advanced encryption standard (AES) with cipher block chaining (CBC). Select from **aes-cbc 128**, **aes-cbc 192**, or **aes-cbc 256**. **des** uses DES.
<*encryption key*>	Specifies the hexadecimal encryption key. The size of the encryption key is determined by the respective encryption algorithm, as follows: **3des** uses a **48** character key size. **aes-cbc 128** uses a **32** character key size. **aes-cbc 192** uses a **48** character key size. **aes-cbc 256** uses a **64** character key size. **des** uses a **16** character key size.
<*authentication type*>	Specifies the algorithm used for authenticating OSPFv3 messages. Valid authentication methods are Message-Digest 5 (**md5**) and Secure-Hash 1 (**sha1**) algorithms.

<authentication key> Specifies the hexadecimal authentication key. The size of the authentication key is determined by the respective authentication algorithm, as follows:

md5 uses a **32** character key size.

sha1 uses a **40** character key size.

Default Values

By default, there is no security for OSPFv3 messages on an interface.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

This commands specifies OSPFv3 security at the interface level. Protection specified with this command overrides any area-level OSPFv3 protection that might apply to the interface.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages with an SPI of **120**, no encryption, and **md5** as the authentication method:

```
(config)#interface vlan 1
(config-interface-vlan 1)#ospfv3 encryption ipsec spi 120 esp null md5
    NeWtStpsswdLoonGpsswDhtThmnWoKEY
```

ospfv3 <*process id*> hello-interval <*value*>

Use the **ospfv3 hello-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) Hello packets sent on the interface. This value must be the same across all interfaces on the link. Use the **no** form of this command to return the Hello packet interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
hello-interval <*value*>	Specifies the number of seconds allowed between OSPFv3 Hello packets. Valid range is **1** to **65535** seconds.

Default Values

By default, the Hello packet interval for OSPFv3 is **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the interval between OSPFv3 Hello packets on the interface is **20** seconds:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 5 hello-interval 20**

ospfv3 <*process id*> network

Use the **ospfv3 network** command to specify the network type for Open Shortest Path First version 3 (OSPFv3) enabled interfaces. Use the **no** form of this command to return the interface's network type to the default value. Variations of this command include:

ospfv3 <*process id*> **network broadcast**
ospfv3 <*process id*> **network point-to-point**

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
broadcast	Specifies that the OSPFv3 network type for the interface is set to broadcast.
point-to-point	Specifies that the OSPFv3 network type for the interface is set to point-to-point.

Default Values

By default, Ethernet interfaces are set to network type broadcast, and point-to-point (PPP), Frame Relay, and loopback interfaces are set to network type point-to-point.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the network interface as point-to-point:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 5 network point-to-point**

ospfv3 <*process id*> priority <*value*>

Use the **ospfv3 priority** command to specify the Open Shortest Path First version 3 (OSPFv3) priority for the interface. Use the **no** form of this command to return the interface's priority to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
priority <*value*>	Specifies the OSPFv3 priority for the interface. Valid range is **0** to **255**.

Default Values

By default, the OSPFv3 priority of an interface is set to **1**.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

Priority is used in the election of the designated router and backup designated router on multi-access networks. Interfaces connected to multi-access networks (such as Ethernet interfaces) perform an election for a designated and backup designated router. The router interface with the highest OSPFv3 priority on the link becomes the designated router for that link. The interface with the next highest priority becomes the designated backup router. In the event there is a tie, the router interface with the highest router ID takes precedence. A priority value of **0** indicates the router is ineligible to become either the designated or backup designated router.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's OSPFv3 priority value to **6**:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 5 priority 6**

ospfv3 <*process id*> retransmit-interval <*value*>

Use the **ospfv3 retransmit-interval** command to specify the interval between Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) sent on the interface. Use the **no** form of this command to return the OSPFv3 LSA interval to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
retransmit-interval <*value*>	Specifies the number of seconds between OSPFv3 LSAs sent on the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA retransmit interval is set to **5** seconds.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the LSA retransmit interval is **10** seconds:

```
(config)#interface vlan 1
(config-interface-vlan 1)#ospfv3 5 retransmit-interval 10
```

ospfv3 <*process id*> shutdown

Use the **ospfv3 shutdown** command to disable an Open Shortest Path First version 3 (OSPFv3) process on the interface. When this command is used, the OSPFv3 commands remain in place, but logically it appears to the interface as though the OSPFv3 process has been removed from the configuration. This command can be useful in troubleshooting. Use the **no** form of this command to reinstate the OSPFv3 process.

Syntax Description

<process id>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.

Default Values

No default values are necessary for this command.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables OSPFv3 process **5** on the interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 5 shutdown**

ospfv3 <*process id*> transmit-delay <*value*>

Use the **ospfv3 transmit-delay** command to specify the estimated time that is required to propagate an Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSA) on the interface. Use the **no** form of this command to return the transmit delay to the default value.

Syntax Description

<*process id*>	Specifies the OSPFv3 routing process this interface is to join. Valid process ID range is **1** to **65535**. If the process ID has not already been created (using the command *ospfv3 <process id> area <area id> on page 3467*), entering this command will not create the ID. Only one OSPFv3 process can be configured at a time; if another OSPFv3 process exists, an error is reported.
transmit-delay <*value*>	Specifies the number of seconds required to send LSAs from the interface. Valid range is **1** to **65535** seconds.

Default Values

By default, the LSA transmit delay is set to **1** second.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the interface's LSA transmit delay to **2** seconds:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#ospfv3 5 transmit-delay 2**

packet-capture <*name*>

Use the **packet-capture** command to apply a previously configured packet capture instance to the interface. Use the **no** form of this command to remove the packet capture instance.

Syntax Description

<*name*>	Specifies the name of the packet capture instance to apply to the interface.

Default Values

By default, no packet capture instances are configured or applied to the interface.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. For more information about packet capturing, its uses, and its implementation in AOS, refer to the configuration guide *Configuring Packet Capture in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example applies the previously configured packet capture **1CAPTURE** to the interface:

(config)**#interface vlan 1**
(config-vlan 1)**#packet-capture 1CAPTURE**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing (WFQ).
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the virtual local area network (VLAN) interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on the virtual local area network (VLAN) interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#rtp quality-monitoring**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.

Usage Examples

The following example enables SNMP capability on the VLAN interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is set to enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release 17.2	Command was expanded to the cellular interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the VLAN interface:

(config)**#interface vlan 1**
(config-interface-vlan 1)**#no snmp trap link-status**

traffic-shape rate <*value*>

Use the **traffic-shape rate** command to specify and enforce an output bandwidth for the virtual local area network (VLAN) interface. Use the **no** form of this command to disable this feature. Variations of this command include:

traffic-shape rate <*value*>
traffic-shape rate <*value*> **count-eth-overhead**
traffic-shape rate <*value*> <*burst*>
traffic-shape rate <*value*> <*burst*> **count-eth-overhead**

Syntax Description

<*value*>	Specifies the rate (in bits per second) at which the interface should be shaped.
<*burst*>	Optional. Specifies the allowed burst in bytes. By default, the burst is specified as the rate divided by 5 and represents the number of bytes that would flow within 200 ms.
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.

Default Values

By default, **traffic-shape rate** is disabled.

Command History

Release 10.1	Command was introduced.
Release R11.1.0	Command was expanded to include the **count-eth-overhead** parameter, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

Traffic shaping can be used to limit the VLAN interface to a particular rate or to specify use of quality of service (QoS).

Usage Examples

The following example sets the outbound rate of **vlan 1** to 128 kbps and applies a QoS policy that gives all Realtime Transport Protocol (RTP) traffic priority over all other traffic:

(config)**#qos map voip 1**
(config-qos-map)**#match ip rtp 10000 10500 all**
(config-qos-map)**#priority unlimited**
(config-qos-map)**#interface vlan 1**
(config-interface-vlan 1)**#traffic-shape rate 128000**
(config-interface-vlan 1)**#qos-policy out voip**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the VLAN interface to the VRF instance named **RED**:

(config)**#interface vlan 1**
(config-vlan1)**#vrf forwarding RED**

vrrp <*number*>

Use the **vrrp** command to configure Internet Protocol version 4 (IPv4) Virtual Router Redundancy Protocol version 2 (VRRPv2) routers within a router group. Use the **no** form of this command to remove the VRRP router's configurations. Variations of this command include:

vrrp <*number*> **description** <*text*>
vrrp <*number*> **ip** <*ipv4 address*>
vrrp <*number*> **ip** <*ipv4 address*> **secondary**
vrrp <*number*> **preempt**
vrrp <*number*> **preempt delay minimum** <*time*>
vrrp <*number*> **priority** <*level*>
vrrp <*number*> **shutdown**
vrrp <*number*> **startup-delay** <*delay*>
vrrp <*number*> **timers advertise** <*interval*>
vrrp <*number*> **timers learn**
vrrp <*number*> **track** <*name*>
vrrp <*number*> **track** <*name*> **decrement** <*value*>

Syntax Description

<*number*>	Specifies the VRRP router group's virtual router ID (VRID) number. Range is **1** to **255**.
description <*text*>	Specifies the textual description of the VRRP router within the group.
ip <*ipv4 address*>	Specifies the IPv4 address to be used by the VRRP router. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
secondary	Optional. Specifies the entry of an additional VRRP router supported IPv4 address.
preempt	Allows a VRRP router to preempt the current master router if its priority level is higher than the current master's.
delay minimum <*time*>	Optional. Specifies a delay (in seconds) before the specified router will attempt to preempt the current master router. Range is **0** to **255** seconds.
priority <*level*>	Specifies the configured priority level of the VRRP router. Range is **1** to **254**.
shutdown	Disables the VRRP router.
startup-delay <*delay*>	Specifies a time delay (in seconds) before a VRRP router becomes active. Range is **0** to **255** seconds.
timers	Specifies the configuration of the VRRP timers.
advertise <*interval*>	Specifies the time (in seconds) between advertisements sent by the master router. Range is **1** to **255** seconds.
learn	Specifies that the backup VRRP router learns the advertisement interval of the master router.
track <*name*>	Specifies a change in priority level of the VRRP router based upon the specified track.
decrement <*value*>	Optional. Specifies the numerical amount to decrement the VRRP's priority level if the track transitions to a FAIL state. Range is **1** to **254**.

Default Values

By default, VRRP is enabled.

By default, a VRRP router will preempt with no additional delay.

The default configured priority for a VRRP router that is either a backup router or not the IP address owner is **100**. The default actual priority of a VRRP router that is the IP address owner is **255**.

By default, startup-delay is enabled with a default value of **35** seconds.

By default, the advertisement interval is **1** second.

By default, the default decrement value is **10**.

Command History

Release 16.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.

Functional Notes

A VRRP router may be part of more than one virtual router group. Although VRRP group VRIDs can be numbered between 1 and 255, only two VRRP routers per interface are supported.

Adtran recommends that the **timers advertise** setting is kept at the default value. If it is necessary to change this setting, ensure that all VRRP routers are configured with the new value, as all VRRP routers in the virtual group must have the same advertisement interval value. It is also recommended that if the **timers learn** function is enabled on one router in a virtual router group, then the **timers learn** function should be enabled on all routers in the group.

When the virtual router's specified IPv4 address is independent of the IPv4 addresses assigned to real interfaces on the VRRP routers, there is no IPv4 address owner. This addressing method is preferred if object tracking will be used to monitor the network connection. The IPv4 address used for the virtual router must be on the same subnet as either the primary or secondary IPv4 addresses assigned to the VRRP router's real interface.

A track must be created before the **vrrp track** command can be issued. Refer to the *Network Monitor Track Command Set on page 4098* for more information on creating tracks. If a VRRP router owns the virtual router IP address, then the VRRP router's priority level cannot be decremented as a result of the track command. If object tracking will be used, it is important that no VRRP router own the virtual router IP address.

Usage Examples

The following example describes a VRRP router within virtual router group **1** as the **Default Master Router**:

(config)**#interface vlan 1**
(config-interface-vlan 1))**#vrrp 1 description Default Master Router**

The following example specifies an IPv4 address of **10.0.0.1** for a VRRP router within virtual router group **1**:

(config)**#interface vlan 1**
(config-interface-vlan 1))**#vrrp 1 ip 10.0.0.1**

The following example specifies that the VRRP router within virtual router group **1** preempts the current master router after a **30** second delay:

(config)**#interface vlan 1**
(config-interface-vlan 1))**#vrrp 1 preempt delay minimum 30**

The following example specifies the configured priority for the VRRP router within virtual router group **1** is **254**:

(config)**#interface vlan 1**
(config-interface-vlan 1))**#vrrp 1 priority 254**

The following example disables the VRRP router within virtual router group **1**:

(config)**#interface vlan 1**
(config-interface-vlan 1))**#vrrp 1 shutdown**

The following example configures a VRRP router on group **1** to delay **45** seconds before becoming active:

(config)**#interface vlan 1**
(config-interface-vlan 1))#vrrp 1 startup-delay 45

vrrpv3 <*vrid*> address-family

Use the **vrrpv3 address-family** command to configure Virtual Router Redundancy Protocol version 3 (VRRPv3) routers on the interface. This command enables VRRPv3, creates a virtual router ID (VRID), and specifies whether you are using Internet Protocol version 4 (IPv4) or IP version 6 (IPv6) VRRPv3. Use the **no** form of this command to remove the VRRPv3 router configuration. Variations of this command include:

vrrpv3 <*vrid*> **address-family ipv4**
vrrpv3 <*vrid*> **address-family ipv6**

Syntax Description

<*vrid*>	Specifies the VRID for the virtual router instance. This value is advertised by VRRPv3 and is used to generate the virtual router medium access control (MAC) address. Valid range is **1** to **255**.
ipv4	Specifies that IPv4 is used with VRRPv3, and enters the virtual router instance's configuration mode.
ipv6	Specifies that IPv6 is used with VRRPv3, and enters the virtual router instance's configuration mode.

Default Values

By default, VRRPv3 is not configured.

Command History

Release R10.11.0	Command was introduced. This command replaces **vrrpv3** <*vrid*> on the interface.

Functional Notes

VRID values must be the same on all routers that are part of the virtual router group. VRID numbering is independent between VRRPv3 IPv4 and IPv6 address families. Once the VRRPv3 VRID is created and the address family is specified, the virtual router instance's configuration mode is entered. Only two VRIDs per interface per IP version are supported. For more information about configuring the VRRPv3 instance, refer to *VRRPv3 Command Set on page 4221*.

Usage Examples

The following example enables IPv4 VRRPv3, creates a VRID of **15** for the instance, and enters the virtual router instance's configuration mode:

(config)**#interface vlan 1**
(config-vlan 1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)#

The following example enables IPv6 VRRPv3, creates a VRID of **6** for the instance, and enters the virtual router instance's configuration mode:

(config)**#interface vlan 1**
(config-vlan 1)**#vrrpv3 6 address-family ipv6**
(config-if-vrrpv3 6)#

WIRELESS INTERFACE COMMAND SETS

This section includes the following command sets:

NETVANTA 150 AP INTERFACE COMMAND SET

The NetVanta 150 Access Point Interface Configuration command set is used to configure wireless access points (APs) connecting to an AOS platform running the Adtran Wireless Control Protocol (AWCP). The AP is either a physical standalone unit (such as the NetVanta 150) or integrated within an AOS platform via a module, also known as an embedded access point module (EAPM).

Enter the **interface dot11ap** *<ap | ap/radio | ap/radio.vap>* **ap-type nv150** command at the Global Configuration mode prompt to activate the NetVanta 150 AP Interface Configuration mode. For example:

```
>enable
#configure terminal
(config)#interface dot11ap 1 ap-type nv150
(config-dot11ap 1)#
```

Additional steps must be performed before the NetVanta 150 AP is ready for connectivity. The radio-level settings are configured using the NetVanta 150 Radio Interface Command Set on page 3510. The virtual access point (VAP) settings are configured using the NetVanta 150 VAP Interface Command Set on page 3533.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

access-point controller-standby on page 3495
access-point mac-address <mac address> on page 3496
association access-list <name> on page 3497
country-region on page 3498
encapsulation 802.1q on page 3500
ethernet-speed on page 3502
event-history on page 3503
full-duplex on page 3504
half-duplex on page 3505
ip address <ipv4 address> <subnet mask> on page 3506
ip default-gateway <ipv4 address> on page 3507
location <name> on page 3508
name <name> on page 3509

access-point controller-standby

Use the **access-point controller-standby** command to release wireless access controller (AC) control of the NetVanta 150 wireless access point (AP). This command will cause the AC to stop responding to echo requests from the AP, releasing control of the AP. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, controller-standby mode is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example enables controller-standby mode for this AP interface:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#access-point controller-standby**

access-point mac-address *<mac address>*

Use the **access-point mac-address** command to specify the medium access control (MAC) address of the NetVanta 150 wireless access point (AP) physical Ethernet interface. Use the **no** form of this command to delete the MAC address of the AP.

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Functional Notes

This command binds the wireless access controller (AC) to the AP. Without specifying the MAC address, the AC cannot control the AP.

Usage Examples

The following example configures an AP MAC address of **00:0A:C8:5F:00:D2**:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#access-point mac-address 00:0A:C8:5F:00:D2**

association access-list <*name*>

Use the **association access-list** command to specify a medium access control (MAC) address filter. This filter will only allow access to specific wireless clients. A MAC access control list (ACL) must be created before it can be associated with this NetVanta 150 wireless access point (AP). Refer to *mac access-list standard <name> on page 1606* for more information. Use the **no** form of this command to remove an associated MAC ACL from this AP.

Syntax Description

<name>	Specifies the name of the previously created MAC ACL.

Default Values

By default, no MAC ACLs are associated with an AP.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example configures the AP to use the MAC ACL named **ALLOWLIST** as a filter for allowing access:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#association access-list ALLOWLIST**

country-region

Use the **country-region** command to specify the country region or domain where the NetVanta 150 wireless access point (AP) is being used so that the radio can modify its settings to conform to that country's regulations. Use the **no** form of this command to return to the default value. Variations of this command include:

country-region Asia
country-region Australia
country-region Canada
country-region Denmark
country-region Europe
country-region Finland
country-region France
country-region Germany
country-region Ireland
country-region Italy
country-region Japan
country-region Mexico
country-region Netherlands
country-region New_Zealand
country-region Norway
country-region Puerto_Rico
country-region South_America
country-region Spain
country-region Sweden
country-region Switzerland
country-region UK
country-region USA

Syntax Description

Asia	Specifies Asia configuration.
Australia	Specifies Australia configuration.
Canada	Specifies Canada configuration.
Denmark	Specifies Denmark configuration.
Europe	Specifies Europe configuration.
Finland	Specifies Finland configuration.
France	Specifies France configuration.
Germany	Specifies Germany configuration.
Ireland	Specifies Ireland configuration.
Italy	Specifies Italy configuration.
Japan	Specifies Japan configuration.
Mexico	Specifies Mexico configuration.
Netherlands	Specifies Netherlands configuration.

New_Zealand	Specifies New Zealand configuration.
Norway	Specifies Norway configuration.
Puerto_Rico	Specifies Puerto Rico configuration.
South_America	Specifies South America configuration.
Spain	Specifies Spain configuration.
Sweden	Specifies Sweden configuration.
Switzerland	Specifies Switzerland configuration.
UK	Specifies UK configuration.
USA	Specifies USA configuration.

Default Values

By default, the country-region is set to **USA**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example sets the country of operation to **Norway**:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#country-region Norway**

encapsulation 802.1q

Use the **encapsulation 802.1q** command to set the NetVanta 150 wireless access point (AP) for virtual local area network (VLAN) encapsulation 802.1q mode. This will apply VLAN tags to the user traffic. Use the **no** form of this command to disable VLAN encapsulation. Variations of this command include:

encapsulation 802.1q
encapsulation 802.1q awcp-vlan <*vlan id*> **native**
encapsulation 802.1q awcp-vlan <*vlan id*> **native priority** <*level*>

Syntax Description

awcp-vlan <*vlan id*>	Optional. Specifies an existing VLAN to be used for Adtran Wireless Control Protocol (AWCP) connection. Valid range is **1** to **4096**. For more information on creating a VLAN, refer to *VLAN Interface Command Set on page 3370*.
native	Enables native mode for the specified VLAN. Packets from this VLAN leaving the interface will not be tagged with the VLAN number. Any untagged packets received by the interface are considered a part of the native VLAN ID. Only one VLAN may be set to **native**. To change where the native VLAN resides, the current native must be disabled using the **no** form of this command before a new one is set.
priority <*level*>	Optional. Specifies the 802.1q priority level for AWCP packets generated by this AP when VLAN tags are applied. Valid range is **1** to **7**, with 1 being the highest priority.

Default Values

By default, **encapsulation 802.1q** is disabled on the AP.

Command History

Release 6.1	Command was introduced.
Release 15.1	Command was expanded to include the access point (AP) interface.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Functional Notes

Settings (including encapsulation, VLAN, and native VLAN) for the AP's Ethernet interface must be coordinated with the physical interface to which the AP is connected.

Since all functions on an AP use the same Ethernet interface, there should be only one VLAN ID set to **native** on the entire AP. It is possible that a VLAN can be used on a virtual access point (VAP) and for the AWCP protocol on the AP’s Ethernet, but this is not typical. Typically, the control protocol will use the native VLAN and the VAP’s data will all be tagged on the Ethernet.

This means that one VLAN on one radio's VAP may be set to **native** or the control protocol (AWCP) VLAN may be set to **native**, but not both unless they both use the same VLAN ID. Typically, the control protocol will use the native VLAN.

If the control protocol and a VAP share the same VLAN ID, control protocol packets will be intercepted by the AP while noncontrol protocol packets will be forwarded to the VAP.

If the AP is to be in trunk mode and the AWCP VLAN is not the native VLAN for the trunk, care must be exercised in transitioning the AP and switchport from access port (nontrunk) mode. The AP should be configured first, then the switchport set to match. When transitioning the AP, set its AWCP VLAN first, then enable trunking mode (encapsulation 802.1q). If the AWCP VLAN is the native VLAN on the AP and switch, AWCP communication will not be lost no matter what combination of trunk mode settings is applied.

Usage Examples

The following example enables encapsulation 802.1q on this AP and makes VLAN 1 the native VLAN:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#encapsulation 802.1q awcp-vlan 1 native**

ethernet-speed

Use the **ethernet-speed** command to configure the speed of the NetVanta 150 wireless access point's (AP) Ethernet interface. Use the **no** form of this command to return to the default value. Variations of this command include:

ethernet-speed 10
ethernet-speed 100
ethernet-speed auto

This command is not available for the embedded access point module (EAPM). For the EAPM, the Ethernet speed is fixed at 100 Mbps.

Syntax Description

10	Configures the AP's Ethernet speed for 10 Mbps.
100	Configures the AP's Ethernet speed for 100 Mbps.
auto	Configures the AP's Ethernet speed for auto negotiation.

Default Values

By default, the **ethernet-speed** is set to **auto**.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets the AP's Ethernet speed to 10 Mbps:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#ethernet-speed 10**

event-history

Use the **event-history** command to configure the NetVanta 150 wireless access point (AP) to transmit log messages to the wireless access controller (AC) via the control protocol. The AC will then integrate these messages into the AC's event subsystem for local display, history, or syslog forwarding. Use the **no** form of this command to terminate log messages. Variations of this command include:

event-history on
event-history priority <*level*>

Syntax Description

on	Enables the AP to send log messages to the AC.
priority <*level*>	Sets the minimum priority level of messages sent to the AC. This setting is provided on a per-AP basis so that the user can control the level of logging traffic that will occur on their network. The levels are: 1 (Alert), 2 (Critical), 3 (Error), 4 (Warning), 5 (Notice), 6 (Informational).

Default Values

By default, event history transmission is disabled and the priority level is **3**. This means that messages with levels 1 through 3 will be sent, and messages with level 4 through 6 will not be sent.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example changes the minimum priority level of the log messages sent to the AC to **6**. This will send all log messages to the AC:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#event-history priority 6**

full-duplex

Use the **full-duplex** command to configure the NetVanta 150 wireless access point (AP) Ethernet interface for full-duplex operation. This allows the interface to send and receive simultaneously. Use the **no** form of this command to return to the default **half-duplex** operation.

This command is not available for the embedded access point module (EAPM). The EAPM is fixed at full-duplex operation.

Syntax Description

No subcommands.

Default Values

By default, all AP Ethernet interfaces are configured for **half-duplex** operation.

Command History

Release 15.1	Command was introduced for the AP interface.

Functional Notes

Full-duplex Ethernet is a variety of Ethernet technology currently being standardized by the IEEE. Because there is no official standard, vendors are free to implement their independent versions of full-duplex operation. Therefore, it is not safe to assume that one vendor's equipment will work with another.

Devices at each end of a full-duplex link have the ability to send and receive data simultaneously over the link. Theoretically, this simultaneous action can provide twice the bandwidth of normal (half-duplex) Ethernet. To deploy full-duplex Ethernet, each end of the link must only connect to a single device. With only two devices on a full-duplex link, there is no need to use the medium access control mechanism (to share the signal channel with multiple stations) and listen for other transmissions or collisions before sending data.

Usage Examples

The following example configures the AP's Ethernet interface for **full-duplex** operation:

(config)**#interface dot11ap 1 ap-type nv1500**
(config-dot11ap 1)**#full-duplex**

half-duplex

Use the **half-duplex** command to configure the NetVanta 150 wireless access point's (AP) Ethernet interface for half-duplex operation. This setting allows the Ethernet interface to either send or receive at any given moment, but not simultaneously. Use the **no** form of this command to disable half-duplex operation.

This command is not available for the embedded access point module (EAPM). The EAPM is fixed at full-duplex operation.

Syntax Description

No subcommands.

Default Values

By default, all Ethernet interfaces are configured for **half-duplex** operation.

Command History

Release 15.1	Command was introduced for the AP interface.

Functional Notes

Half-duplex Ethernet is the traditional form of Ethernet that employs the carrier sense multiple access/collision detect (CSMA/CD) protocol to allow two or more hosts to share a common transmission medium while providing mechanisms to avoid collisions. A host on a half-duplex link must listen on the link, and only transmit when there is an idle period. Packets transmitted on the link are broadcast (so it will be heard by all hosts on the network). In the event of a collision (two hosts transmitting at once), a message is sent to inform all hosts of the collision and a backoff algorithm is implemented. The backoff algorithm requires the station to remain silent for a random period of time before attempting another transmission. This sequence is repeated until a successful data transmission occurs.

Usage Examples

The following example configures the AP Ethernet interface for **half-duplex** operation:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#half-duplex**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address for the NetVanta 150 access point (AP) Ethernet interface. Use the **no** form of this command to remove a configured IPv4 address.

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 15.1	Command was introduced for the AP interface.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Functional Notes

The IPv4 address and subnet mask are only needed on the AP interface if the user wants to use remote authentication dial-in user service (RADIUS) authentication with the wireless clients. A default gateway may also need to be specified.

Usage Examples

The following example configures an IPv4 address of **192.22.72.101** and a subnet mask of **255.255.255.252**:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#ip address 192.22.72.101 255.255.255.252**

ip default-gateway *<ipv4 address>*

Use the **ip default-gateway** command to assign a default gateway to the NetVanta 150 wireless access point (AP). This allows the AP to communicate with Internet Protocol version 4 (IPv4) devices on other IPv4 subnets. Use the **no** form of this command to remove the default gateway.

Syntax Description

<ipv4 address>	Specifies the default gateway IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there is no configured default gateway.

Command History

Release 15.1	Command was introduced for the AP interface.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example assigns the AP a default gateway for **10.10.10.1**:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#ip default-gateway 10.10.10.1**

location *<name>*

Use the **location** command to specify the location of the NetVanta 150 wireless access point (AP). Use the **no** form of this command to remove the specified location.

Syntax Description

<name>	Specifies the name of the location of the AP. The location name may be up to 32 characters.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example assigns the name **FLOOR5** as the location of AP 1:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#location FLOOR5**

name <*name*>

Use the **name** command to specify a name for this NetVanta 150 wireless access point (AP). Use the **no** form of this command to remove the assigned name.

Syntax Description

<*name*>	Specifies the name of the AP. The name may be up to 32 characters in length.

Default Values

By default, the name of the AP will be ADTN plus the last three bytes of the AP medium access control (MAC) address (all uppercase).

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example assigns the name **ACCOUNTING1** to AP 1:

(config)**#interface dot11ap 1 ap-type nv150**
(config-dot11ap 1)**#name ACCOUNTING1**

NETVANTA 150 RADIO INTERFACE COMMAND SET

A NetVanta 150 radio interface is a virtual interface that can be programmed into an AOS platform running the Adtran Wireless Control Protocol (AWCP). This interface is used to configure radio-level commands for an 802.11 wireless access point (AP). The AP is either a physical standalone unit (such as the NetVanta 150) or integrated within the AOS platform via a module, also known as an embedded access point module (EAPM).

The associated AP interface must be configured before access to the Radio Interface Configuration mode is possible. For more information on configuring the AP, refer to *NetVanta 150 AP Interface Command Set on page 3494*. Upon creation, each radio will have one default virtual access point (VAP) configured. More detailed information on configuring the VAP interface is provided in *NetVanta 150 VAP Interface Command Set on page 3533*.

There are only two radio types: 802.11a and 802.11bg. Radio 802.11bg defaults to **interface dot11ap** <*ap*/**1**> and radio 802.11a defaults to **interface dot11ap** <*ap*/**2**>. The only changes that can be made to the radio types is to specify the radio mode of the 802.11bg radio as type b, g, or bg using the command *radio-mode on page 3523*.

The parent (AP) interface must be created before access to the Radio Interface Configuration mode is possible. Execute the ***interface dot11ap*** *<ap> command to create an AP interface.*

To activate Radio Interface Configuration mode for an 802.11b or g radio, enter the commands at the Global Configuration mode prompt as shown below:

```
>enable
#configure terminal
(config)#interface dot11ap 1/1
(config-dot11ap 1/1-bg)#
```

To activate Radio Interface Configuration mode for an 802.11a radio, enter the commands at the Global Configuration mode prompt as shown below:

```
>enable
#configure terminal
(config)#interface dot11ap 1/2
(config-dot11ap 1/2-a)#
```

By default, ***interface dot11ap*** *<ap/**1**> is radio type 802.11bg and* ***interface dot11ap*** *<ap/**2**> is radio type 802.11a.*

*Not all radio interface commands apply to both radio types.Use the **?** command to display a list of valid commands.*

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

antenna

Use the **antenna** command to select the desired antenna mode. Use the **no** form of this command to return to the default value. Variations of this command include the following:

antenna 1
antenna 2
antenna diversity

Syntax Description

1	Sets the antenna mode to transmit or receive on antenna 1.
2	Sets the antenna mode to transmit or receive on antenna 2.
diversity	Sets the mode to transmit or receive on antenna with best signal.

Default Values

By default, the antenna is set to **diversity**.

Command History

Release 15.1	Command was introduced.

Functional Notes

Diversity antennas are two separate antennas that are attached to a single wireless radio. These antennas are designed to reduce the effects of multi-path radio distortion. Each antenna samples the radio signal around the access point (AP). The antenna receiving the best signal is chosen to transmit and receive information. Only one diversity antenna is in use at any given time.

Usage Examples

The following example sets the antenna mode to transmit or receive on antenna 1 on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#antenna 1**

beacon period *<time>*

Use the **beacon period** command to set the time between beacons. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the number of 802.11 time units (TUs) between beacons. One TU is 1024 microseconds. Range is **20** to **1000** TU.

Default Values

By default, the beacon period is **100** TU.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

A beacon is a type of management frame used in 802.11 wireless networks. Beacon frames carry important information, such as the basic service set, parameter sets, and capability. The beacon frame is sent to the broadcast medium access control (MAC) address, which means that all clients must be able to receive and process beacons.

Beacon frames are associated with some overhead, which decreases the throughput of the wireless network. The higher the beacon period, the fewer number of beacons sent, thus reducing overhead and increasing throughput on the network. However, fewer beacons can cause a delay in the association process because stations scanning for available access points (APs) may miss the beacons.

Usage Examples

The following example sets the beacon period to 500 TU on an 802.11 bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#beacon period 500**

channel <*number*>

Use the **channel** command to manually select a channel for the wireless radio or to scan for the best channel available. Use the **no** form of this command to return to the default value. Variations of this command include the following:

channel <*number*>
channel least-congested

Syntax Description

<*number*>	Specifies the Institute of Electrical and Electronics Engineers, Inc. (IEEE) channel number. The range of channels is dependent on the radio type and country setting
least-congested	Sets the radio to scan for the best channel available.

Default Values

By default, the radio scans for the least-congested channel available.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Note

*Type **channel ?** to display a list of valid channels from which to choose. The list of channels displayed is based on the selected radio type (refer to the command radio-mode on page 3523) and country setting (refer to the command country-region on page 3498).*

Usage Examples

The following example manually sets an 802.11bg wireless radio to channel 6 in the United States:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#channel 6**

The following example manually sets an 802.11a wireless radio to channel 149 in the United States:

(config)**#interface dot11ap 1/2 radio-type 802.11a**
(config-dot11ap 1/1-a)**#channel 149**

fragment-threshold *<length>*

Use the **fragment-threshold** command to set the packet length threshold. Packets larger than the value set in this command will be fragmented when transmitted on the wireless link. Use the **no** form of this command to return to the default value.

Syntax Description

<length>	Specifies the maximum packet length allowed before fragmentation will occur. Range is **256** to **2346** bytes.

Default Values

By default, the fragment threshold is set at **2346** bytes.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

The fragment threshold can be set to a lower number to prevent retransmission of large packets, but the overhead will increase. If the threshold is large, the overhead is relatively small but large packets will be retransmitted, lowering efficiency.

Usage Examples

The following example sets the fragment threshold at **572** bytes on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#fragment-threshold 572**

inactivity-timeout max <*value*>

Use the **inactivity-timeout max** command to set the maximum length of inactivity allowed between an access point (AP) and its clients. If no response is seen from the client within the timeout, the client will be disassociated. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the maximum length of time a connection between an AP and a client is allowed to remain inactive. Range is **1** to **99** minutes.

Default Values

By default, the maximum inactivity timeout is **5** minutes.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Usage Examples

The following example sets the maximum inactivity timeout to **2** minutes on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#inactivity-timeout max 2**

power local

Use the **power local** command to select the radio's transmit power level. The range of the power level is relative to the country region currently specified for the radio. Use the **no** form of this command to return to the default value. Variations of this command include:

power local eighth
power local half
power local maximum
power local minimum
power local quarter

Syntax Description

eighth	Sets the power local level to one-eighth of the maximum output power setting.
half	Sets the power local level to one-half of the maximum output power setting.
maximum	Sets the power local level to the maximum output power setting.
minimum	Sets the power local level to the minimum output power setting.
quarter	Sets the power local level to one-fourth of the maximum output power setting.

Default Values

By default, the power local setting is **maximum**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

Radio cell size and interference between cells can be reduced by lowering the radio's transmit power level.

Usage Examples

The following example sets the radio's transmit power to one-half maximum power on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#power local half**

preamble-short

Use the **preamble-short** command to enable short preamble mode on an 802.11bg radio. The preamble is information at the beginning of a packet that is used by the access point (AP), as well as its clients. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, short preamble mode is enabled.

Command History

Release 15.1	Command was introduced.

Functional Notes

When short preamble mode is enabled, clients may request short or long preambles according to need. Disabling short preamble mode means that clients must request long preambles only.

Short preamble mode is not supported on the 5 GHz 802.11a radio.

Usage Examples

The following example enables short preamble mode on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#preamble-short**

protection-mode

Use the **protection-mode** command to configure the protection mode, type, and rate for an 802.11bg radio. Use the **no** form of this command to return to the default value. Variations of this command include the following:

protection-mode always
protection-mode always type cts-only
protection-mode always type cts-only rate 1
protection-mode always type cts-only rate 2
protection-mode always type cts-only rate 5.5
protection-mode always type cts-only rate 11
protection-mode always type rts-cts
protection-mode always type rts-cts rate 1
protection-mode always type rts-cts rate 2
protection-mode always type rts-cts rate 5.5
protection-mode always type rts-cts rate 11
protection-mode auto
protection-mode auto type cts-only
protection-mode auto type cts-only rate 1
protection-mode auto type cts-only rate 2
protection-mode auto type cts-only rate 5.5
protection-mode auto type cts-only rate 11
protection-mode auto type rts-cts
protection-mode auto type rts-cts rate 1
protection-mode auto type rts-cts rate 2
protection-mode auto type rts-cts rate 5.5
protection-mode auto type rts-cts rate 11

This command is only available on the 802.11bg radio interface.

Syntax Description

always	Protection mode is always on regardless of the presence of 802.11b clients.
auto	Protection mode is automatically activated when an 802.11b client associates with an 802.11g access point (AP).
type	
cts-only	Specifies clear to send-only (CTS-only) protection mode.
rts-cts	Specifies request to send-clear to send (RTS-CTS) protection mode.
rate	
1	Sets the packet rate to 1 Mbps.
2	Sets the packet rate to 2 Mbps.

5.5	Sets the packet rate to 5.5 Mbps.
11	Sets the packet rate to 11 Mbps.

Default Values

By default, **protection-mode** is set to **auto**, **type** is set to **cts-only**, and the **rate** is set to **11**.

Command History

Release 15.1	Command was introduced

Functional Notes

Protection mode is used when 802.11b and 802.11g radios exist together on the same wireless local area network (WLAN) network. 802.11g devices are required to be backwards-compatible with legacy 802.11b devices. Both radios operate in the 2.4 GHz frequency range; however, each uses a different transmission type. 802.11b radios use direct sequence spread spectrum (DSSS) for transmitting data, and 802.11g radios use orthogonal frequency division multiplexing (OFDM) for transmitting data. Contention for media access on 802.11 networks is managed via carrier sense multiple access with collision avoidance (CSMA/CA), but the use of two different transmission types prevents 802.11b devices from hearing transmission attempts on the shared radio frequency (RF) medium. Protection mode addresses this problem and allows for coexistence of 802.11b and 802.11g devices on a network.

There are two protection mode types: CTS-only, also known as CTS-to-self, and RTS-CTS. Both types are used when an 802.11g AP associates with an 802.11b client. Compared to a network that contains solely 802.11g clients, use of a protection mode reduces throughput. Compared to each other, CTS-only mode requires slightly less protocol overhead than RTS-CTS mode. Protection frames must be transmitted at 802.11b rates (1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps) to ensure these frames are received and processed by all clients on the network.

During CTS-only mode, clients that have a frame for transmission on the RF medium will first transmit a CTS frame. The destination address specified in this CTS frame is the transmitting client's own medium access control (MAC) address. All clients connected to the RF medium are required to listen to CTS frames. A CTS frame is interpreted as a *do not send* command by all clients except by the one whose MAC address is specified in the destination field.

When RTS-CTS is employed, clients must request access to the RF medium by sending an RTS to the AP. The client refrains from accessing the medium and transmitting data until it receives a CTS from the AP. A CTS command is interpreted as a *do not send* command when it is received by a client that did not initiate the RTS. RTS-CTS requires more protocol overhead than CTS-only.

Usage Examples

The following example enables protection mode to automatically activate upon association of an 802.11b client with an 802.11g AP. RTS-CTS is specified, but the rate is not. This means that the default rate of 11 Mbps will be used.

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#protection-mode auto type rts-cts**

qos-mode wmm

Use the **qos-mode wmm** command to enable WiFi multimedia (WMM) quality of service (QoS) mode. Use the **no** form of this command to disable WMM mode. Variations of this command include the following:

qos-mode wmm
qos-mode wmm no-ack

Syntax Description

no-ack	Optional. Specifies the no acknowledgements be sent.

Default Values

By default, WMM QoS mode is disabled.

Command History

Release 15.1	Command was introduced.

Functional Notes

AOS supports WMM, which adds QoS functionality to the wireless network. QoS helps control the allocation of bandwidth on the wireless local area network (WLAN). The benefits of QoS may not be noticed if the traffic load on the wireless network is light. However, QoS benefits will become more apparent as the traffic load on the WLAN increases.

WMM in AOS is based on the enhanced distributed channel access (EDCA) method. This method ensures that higher priority traffic has a better chance of being transmitted on the WLAN than lower priority traffic. There are four priority classes defined in WMM to manage traffic from different applications: voice, video, best-effort, and background. According to algorithms defined in EDCA, a client with traffic in a higher priority class, such as voice, will typically back off of the radio frequency (RF) medium for a shorter period of time than a client with traffic in a lower priority class, such as email. In addition, each priority class is assigned a transmit opportunity (TXOP), which is a set amount of time during which a client can send as many frames as possible. Higher priority classes are given a longer TXOP interval than lower priority classes.

WMM must be enabled on both the access points (APs) and the clients running applications that require QoS. These applications must be able to support WMM for the QoS functionality to be used. In addition, the applications must be capable of assigning the appropriate priority class to their generated streams of traffic.

When acknowledgements are enabled, transmission is more reliable because an acknowledge frame is returned for every frame received. However, acknowledgement frames increase the amount of traffic on the WLAN, which results in decreased performance. Disabling acknowledgements means that transmission will not be as reliable, but performance will be better. For example, having no acknowledgements would be useful for voice traffic because the speed of transmission is most important and packet loss to a certain degree is tolerable.

Usage Examples

The following example enables WMM QoS mode without acknowledgements on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#qos-mode wmm no-ack**

radio-mode

Use the **radio-mode** command to set a specific radio type. Use the **no** form of this command to return to the default value. Variations of this command include the following:

radio-mode a
radio-mode b
radio-mode bg
radio-mode g

Syntax Description

a	Specifies radio type a.
b	Specifies radio type b.
bg	Specifies radio type g in backwards-compatible mode to radio type b.
g	Specifies radio type g.

Default Values

By default, the 802.11bg radio is set to **radio-mode bg** and the 802.11a radio is set to **radio-mode a**.

Command History

Release 15.1	Command was introduced.

Functional Notes

Adtran currently supports three of the IEEE 802.11 wireless local area network (WLAN) standards: 802.11a, 802.11b, and 802.11g. Each access point (AP) contains two integrated radios: one that supports 802.11a and one that supports 802.11b and/or 802.11g.

802.11b is a legacy protocol operating at 2.4 GHz with a maximum throughput of 11 Mbps. This throughput value is derived from the use of direct sequence spread spectrum (DSSS) technology for transmission. The North American channel set contains 11 channels, each 22 MHz wide. Out of these 11 channels, there are only three nonoverlapping or noninterfering channels. The use of three discreet access points (APs) in the same area, each set to one of the three nonoverlapping channels, will result in an aggregate bandwidth of 33 Mbps. The theoretical maximum distance for 802.11b is 100 meters. However, the actual distance is approximately 60 meters in a typical office environment.

802.11g operates at 2.4 GHz with a maximum throughput of 54 Mbps. The obvious benefit to using 802.11g over 802.11b is faster data transmission. The higher maximum throughput is achieved by using orthogonal frequency division multiplexing (OFDM) in addition to DSSS for transmission. 802.11g is backwards-compatible to 802.11b, helping to ease migration from an existing 802.11b network to an 802.11g network. However, the maximum throughput for an 802.11g network is reduced when operating in backwards-compatibility mode with 802.11b. The North American channel set for 802.11g contains 11 channels, each 22 MHz wide. Out of these 11 channels, there are only three nonoverlapping or noninterfering channels. The use of three discreet APs in the same area, each set to one of the three nonoverlapping channels, will result in an aggregate bandwidth of 162 Mbps. The theoretical maximum distance for 802.11g is 100 meters. However, the actual distance is approximately 75 meters in a typical office environment.

802.11a operates at 5.8 GHz with a maximum throughput of 54 Mbps. OFDM is used for transmission. The North American channel set for 802.11 is derived from the lower channels, UNII-1 and UNII-2, in the 5.8 GHz frequency range. There are eight nonoverlapping or noninterfering channels, each 33 MHz wide. The use of eight discreet APs in the same area, each set to one of the eight nonoverlapping channels, will result in an aggregate bandwidth of 432 Mbps. The theoretical maximum distance for 802.11a is 50 meters. However, the actual distance is approximately 25 meters in a typical office environment. 802.11a is not compatible with 802.11b or g.

The data rate associated with any of the radios will continue to drop as a user moves farther away from the AP. The highest data rates will be achieved in areas closest to the AP.

Usage Examples

The following example sets the radio mode to radio type **g** only on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#radio-mode g**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example enables RTP quality monitoring on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#rtp quality-monitoring**

rts threshold *<length>*

Use the **rts threshold** command to set the threshold for use of request to send (RTS) frames. RTS is used to gain access to the radio frequency (RF) medium when long frames need to be transmitted. The RTS threshold defines the minimum long frame length that will require RTS/clear to send (CTS) prior to transmission. Any frame that matches or is longer than the length specified in the **rts threshold** command must be preceded by a RTS/CTS on the RF medium. Use the **no** form of this command to return to the default value.

Syntax Description

<length>	Specifies the length of the RTS threshold in bytes. Range is **256** to **2346** bytes.

Default Values

By default, the RTS threshold is **2346** bytes.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

Generally, it is best to set the RTS threshold as high as possible. However, the threshold may need to be set lower if network throughput is sluggish or there are a high number of frame retransmissions.

Usage Examples

The following example sets the RTS threshold to **1024** bytes on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#rts threshold 1024**

short-slot-time

Use the **short-slot-time** command to enable short slot time (9 microseconds) for an 802.11bg radio. Use the **no** form of this command to return to the long slot time (20 microseconds).

This command is only available on the 802.11bg radio interface.

Syntax Description

No subcommands.

Default Values

By default, **short-slot-time** is enabled.

Short slot time is used only when the wireless network contains strictly 2.4 GHz, 802.11g devices and all of those devices support short slot time. If not all 802.11g devices support short slot time or the wireless network contains both 802.11b and g radios and/or clients, the radio automatically reverts to standard slot time.

Command History

Release 15.1	Command was introduced.

Functional Notes

Slot time is the amount of time a wireless device waits after a collision before retransmitting a packet. The standard slot time of 20 microseconds is used in 2.4 GHz, 802.11b and 802.11bg networks. If a wireless network is strictly 802.11g and all devices are capable of supporting the feature, short slot time (9 microseconds) can be enabled. Short slot time increases throughput by decreasing the backoff time calculated by the transmitting device when a collision occurs.

Usage Examples

The following example specifies use of long slot time for 802.11g exclusive networks on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#no short-slot-time**

speed

Use the **speed** command to set the active rate for the radio. Frames cannot be transmitted at a speed that is higher than the specified active rates. Use the **no** form of this command to return to the default value. Variations of this command include the following:

speed best
speed <*speed*>

Syntax Description

best	Sets the transmit speed of the radio to the best available.
<*speed*>	Sets the transmit speed of the radio. Available speeds vary based on the setting in the **radio-mode** command. For 802.11a radios, choose from 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. For 802.11b radios, choose from 1, 2, 5.5, or 11 Mbps. For 802.11bg radios, choose 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps. For 802.11g radios, choose 6, 9, 12, 18, 24, 36, 48, or 54 Mbps.

*The **speed** setting **best** is recommended.*

Default Values

By default, the active rate is set to **best**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Usage Examples

The following example sets the active rate to **best** on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#speed best**

speed default basic-set

Use the **speed default basic-set** command to configure the basic rate set for the radio. A client connecting to the radio must be able to support these rates. Use the **no** form of this command to return to the default basic rate set for the radio type. Variations of this command include the following:

speed default basic-set 802.11
speed default basic-set 802.11b
speed default basic-set 802.11g
speed default basic-set ofdm

Syntax Description

802.11	Speed for 802.11 (1, 2 Mbps).
802.11b	Speed for 802.11b (1, 2, 5.5, 11 Mbps).
802.11g	Speed for 802.11bg (protection mode) (1, 2, 5.5, 6, 11, 12, 24 Mbps).
ofdm	Speed for orthogonal frequency division multiplexing (OFDM) (6, 12, 24 Mbps).

The OFDM basic rate set on an 802.11bg radio should be specified for a network that only contains 802.11g access points (APs) and clients. This setting maximizes throughput for 802.11g networks, but will not allow 802.11b clients to associate with the access point (AP).

Default Values

By default, the 802.11bg radio is set to **802.11b** and the 802.11a radio is set to **ofdm**.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets the basic rate set for **802.11bg** (protection mode that supports 802.11b and g clients) on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#speed default basic-set 802.11g**

station-role access-point

Use the **station-role access-point** command to set the radio operation mode to access point (AP). Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, the station role is set to **access-point**.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets the station role to **access-point** on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#station-role access-point**

vap-isolation

Use the **vap-isolation** command to enable virtual access point (VAP) isolation, which prevents clients from one VAP on a radio from directly accessing clients in another VAP on the same radio. Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, VAP isolation is disabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example enables VAP isolation an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#vap-isolation**

world-mode dot11d

Use the **world-mode dot11d** command to enable 802.11d mode. This mode allows country codes to be transmitted in beacons sent from the access point (AP). Use the **no** form of this command to disable 802.11d mode.

Syntax Description

No subcommands.

Default Values

By default, **802.11d** mode is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Usage Examples

The following example enables 802.11d mode on an 802.11bg wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#world-mode dot11d**

NETVANTA 150 VAP INTERFACE COMMAND SET

The NetVanta 150 Virtual Access Point (VAP) Interface Configuration command set is used to configure service set identifiers (SSIDs) security and other parameters for each VAP.

A VAP is a logical entity that can exist within a physical wireless access point (AP). VAPs are virtual interfaces represented on wireless networks through the use of a wireless access controller (AC) running the Adtran Wireless Control Protocol (AWCP) and an AP. Each physical AP can support up to eight VAPs for each of the two radio bands for a total of 16 VAPs. VAPs are distinguished by an SSID and can be mapped to a virtual local area network (VLAN). VLAN information can be shared across switches with Ethernet trunks. A common configuration has two VAPs, one associated to a corporate VLAN, and one associated to a guest VLAN.

The associated AP and radio interfaces must be configured before attempting to configure the VAP. For more information on configuring the AP and radios, refer to *NetVanta 150 AP Interface Command Set on page 3494* and *NetVanta 150 Radio Interface Command Set on page 3510*. Each radio will have one default VAP configured. The VAP name is based on the interface to which the AP and radio are mapped using the following syntax, **interface dot11ap** *<ap/radio.vap>*.

To add a VAP or to enter its interface configuration mode, enter the **interface dot11ap** *<ap/radio.vap>* command identifying the appropriate AP and radio interface, followed by the VAP interface number. This command can be entered from the Global Configuration mode prompt or from any other interface configuration mode prompt. In the following example, VAP 1 is created for AP 1 with an 802.11b/g radio.

For example:

```
>enable
#configure terminal
(config)#interface dot11ap 1/1.1
(config-dot11ap 1/1.1-bg)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

accounting on page 3535
client-separation on page 3537
radius-server host on page 3538

accounting

Use the **accounting** command to enable remote authentication dial-in user service (RADIUS) accounting for associations with this virtual access point (VAP) and specify update intervals. Use the **no** form of this command to disable accounting for this VAP. Variations of this command include:

accounting enabled
accounting update
accounting update newinfo
accounting update periodic
accounting update periodic <*value*>

Syntax Description

enabled	Enables RADIUS accounting on this VAP.
update	Defines the RADIUS accounting update setting. Executing the **accounting update** command without specifying any further parameters will send updates when new information occurs. This is the same as executing the **accounting update newinfo** command.
newinfo	Specifies sending RADIUS accounting records as they occur.
periodic	Specifies collecting accounting records and sending them periodically. The default value is **5**.
<*value*>	Optional. Specifies the number of minutes between periodic accounting updates. Valid range is **1** to **99**.

Default Values

By default, RADIUS accounting is disabled.

Functional Notes

The RADIUS server host, access point (AP) IP address, and IP gateway must be configured on the access point for this feature to work. Refer to *radius-server host on page 3538*, *ip address <ipv4 address> <subnet mask> on page 3506*, and *ip default-gateway <ipv4 address> on page 3507* for more information on configuring these parameters.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example enables RADIUS accounting for associations with this VAP:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#accounting enabled**

The following example enables sending RADIUS accounting updates as they occur for this VAP:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#accounting update newinfo**

client-separation

Use the **client-separation** command to prevent wireless clients within this virtual access point (VAP) from communicating directly with each other. Use the **no** form of this command to disable this feature, allowing clients to communicate with one another. It is recommended to enable this command.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example prevents wireless clients on this VAP interface from communicating directly with each other:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#client-separation**

radius-server host

Use the **radius-server host** command to specify the parameters for a remote authentication dial-in user service (RADIUS) server to be used when sending RADIUS messages from the virtual access point (VAP). At a minimum, the Internet Protocol version 4 (IPv4) address of the server must be given. The other parameters are also allowed and (if not specified) will use default values or fall back on the global RADIUS server's default settings. Use the **no** form of this command to remove the RADIUS server properties. This prevents the VAP from using authentication, authorization, and accounting (AAA) methods. Variations of this command include:

radius-server host <*ipv4 address*> **acct-port** <*port*> **auth-port** <*port*> **key** <*key*>
radius-server host <*ipv4 address*> **acct-port** <*port*> **key** <*key*>
radius-server host <*ipv4 address*> **auth-port** <*port*> **acct-port** <*port*> **key** <*key*>
radius-server host <*ipv4 address*> **auth-port** <*port*> **key** <*key*>
radius-server host <*ipv4 address*> **key** <*key*>

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address for the RADIUS server. IPv4 address should be expressed in dotted decimal notation (for example, **10.10.10.1**).
acct-port	Specifies the remote port to which to send accounting requests.
auth-port	Specifies a remote port to which to send authentication requests.
<*port*>	Specifies a User Datagram Protocol (UDP) port number to be used when sending authentication or accounting information to the RADIUS server. Valid range is **1** to **65535**.
key <*key*>	Defines the shared key used between the RADIUS server and the access point. The key must appear last on the input line since it reads the rest of the line beyond the **key** keyword. The maximum length is 64 bytes.

Default Values

By default, a RADIUS server is not defined. The default setting for **acct-port** is **1813** and for **auth-port** is **1812**. By default, no **key** is configured. The IPv4 address in this command refers to the default virtual routing and forwarding (VRF) instance only.

Command History

Release 15.1	Command was expanded to include the VAP interface.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example defines the RADIUS server parameters with an IPv4 address of **10.10.10.1**, sets the accounting port to **1646**, and configures the shared key as **ABC123**:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#radius-server host 10.10.10.1 acct-port 1646 key ABC123**

security mode

Use the **security mode** command to configure the security mode settings for this virtual access point (VAP). Use the **no** form of this command to return to the default setting. Depending on the mode chosen between wired equivalency privacy (WEP) and wi-fi protected access (WPA), further command options are available. Variations of this command include:

security mode none
security mode wep open-key
security mode wep open-key eap
security mode wep open-key eap md5-static-key
security mode wep open-key eap md5-static-key-optional
security mode wep shared-key
security mode wpa aes-ccmp eap
security mode wpa aes-ccmp psk *<key>*
security mode wpa aes-ccmp tkip eap
security mode wpa aes-ccmp tkip psk *<key>*
security mode wpa tkip aes-ccmp eap
security mode wpa tkip aes-ccmp psk *<key>*
security mode wpa tkip eap
security mode wpa tkip psk *<key>*

Adtran does not recommend using the WEP security mode because it is not as secure as WPA.

In order to connect to the access point (AP), a client must support the same security mode as configured on this VAP.

Syntax Description

none	Specifies that no security be used on this VAP. There is no authentication required to connect to this VAP and no encryption is provided on the wireless connection.
wep	Configures the VAP for WEP security mode.
open-key	Specifies that the WEP security mode use open authentication with static WEP keys. The client and the VAP must be configured with the same static key. A static WEP key is configured on the VAP by using the command *security wep-key on page 3542*.
shared-key	Specifies that the WEP security mode use shared authentication with encrypted static keys. The client and the VAP must be configured with the same static key. A static WEP key is configured on the VAP by using the command *security wep-key on page 3542*.

eap	Specifies that the WPA security mode use the Extensible Authentication Protocol (EAP) as a universal authentication framework in the wireless network. A client must support WEP with 802.1x. Authentication is performed between the client and a remote authentication dial-in user service (RADIUS) server.
eap md5-static-key	Defines the WEP security mode for this VAP. A client must support WEP with 802.1x. Authentication is performed between the client and a RADIUS server. It indicates that all clients are using EAP-type message digest 5 (MD5). This EAP type does not perform key generation and requires appropriate static WEP keys be configured on this VAP (refer to *security wep-key on page 3542*). The user can specify security WEP keys 2 through 4, the first WEP key is obtained from the RADIUS server.
eap md5-static-key-optional	Defines the WEP security mode for this VAP. A client must support WEP with 802.1x. Authentication is performed between the client and a RADIUS server. It indicates that some clients are using EAP-type MD5 while other clients are using more advanced EAP types (transport layer security (TLS), Protected Extensible Authentication Protocol (PEAP), etc.). Unlike the advanced EAP types, EAP-type MD5 does not perform key generation and requires appropriate static WEP keys be configured on this VAP (refer to *security wep-key on page 3542*). The user can specify security WEP keys 2 through 4, the first WEP key is obtained from the RADIUS server.
wpa	Configures this VAP for WPA security mode.
aes-ccmp	Specifies using the WPA2 algorithms. This security setting can be used alone or in combination with Temporal Key Integrity Protocol (TKIP).
tkip	Specifies that the WPA security mode use TKIP as its keying structure. This protocol specifies the algorithms used for rotating keys. TKIP can be used alone or in combination with **aes-ccmp**.
psk	Specifies that the WPA security mode use preshared keys (PSKs) for key management. PSK may be used in combination with **tkip** and/or **aes-ccmp**. This method does not require a RADIUS authentication server. The PSK must be known on all VAP clients.
<key>	Defines the PSK for security. The key must consist of 8 to 63 ASCII or 16 to 126 hexadecimal characters. Clients supporting WPA PSK are allowed to connect to this VAP.

Default Values

By default, no security mode is defined.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example shows a typical configuration of these parameters:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security mode wpa tkip psk myPresharedKey**

security wep-key

Use the **security wep-key** command to define the wired equivalency privacy (WEP) keys for use in **wep shared-key** and **wep open-key** security modes (refer to the command *security mode on page 3539*). Up to four keys can be programmed. Set these keys before selecting the WEP security mode. Use the **no** form of this command to disable the specified key. Variations of this command include:

security wep-key *<index> <key>*
security wep-key *<index> <key>* **transmit-key**

*Specifying **security mode wep open-key eap** does not require any WEP keys to be defined on the virtual access point (VAP).*

Syntax Description

<index>	Indicates the WEP key index value. The value and order of WEP-static keys must match on the access point (AP) and all connecting clients. Valid entries are **1** to **4** for **wep shared-key** and **wep open-key**. For **eap md5-static-key** and **eap md5-static-key-optional** modes, the user can specify **security wep-key 2** through **security wep-key 4**, the first WEP key is obtained from the remote authentication dial-in user service (RADIUS) server.
<key>	Specifies the WEP key in hexadecimal characters. The key size is determined using the command *security mode on page 3539* for **wep shared-key** or **wep open-key** security. The key length must follow the setting of the *security wep-key-length on page 3545*.
transmit-key	Enables the specified key to encrypt all wireless traffic sent by this VAP. Only one WEP key index can be the current transmit key. The first index entered under a VAP becomes the transmit key by default. The most recent index specified with the **transmit-key** keyword becomes the current transmit key. The default is the first WEP key index entered for the VAP.

Default Values

By default, no keys are defined.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Functional Notes

The client and the AP must be configured with the same static key.

The corresponding number of hexadecimal or ASCII characters required is:

AP WEP Key Size	Hexadecimal Characters	ASCII Characters
40	10	5
104	26	13
128	32	16

The addition of 24-bit initialization vector (IV) makes the 40 bits become 64 bits, 104 bits become 128, and 128 bits become 152 on the client.

Usage Examples

The following example creates a static WEP key at index **2** with a hexadecimal value of **343f49546a**:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**# security wep-key 2 343f49546a**

security wep-key generate

Use the **security wep-key generate** command to generate wired equivalency privacy (WEP) keys for **shared-key** and **wep open-key** security modes (refer to the command *security mode on page 3539*). Up to four keys can be generated from the passphrase entered using the command *security wep-key seed <passphrase> on page 3546*.

Syntax Description

No subcommands.

Default Values

By default, no keys are defined or generated.

Command History

Release 17.2	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Functional Notes

The generation of WEP keys occurs through the use of a standard message digest 5 (MD5) key generator. The generator creates secure WEP keys by assigning random values for each element (letters or numbers) in the passphrase entered using the command *security wep-key seed <passphrase> on page 3546*.

Usage Examples

The following example enables WEP key generation on 802.11bg wireless radio virtual access point (VAP) 1 based on the passphrase **Adtran6808**:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security wep-key seed Adtran6808**
(config-dot11ap 1/1.1-bg)**#security wep-key generate**

security wep-key-length

Use the **security wep-key-length** command to specify the length of the wired equivalency privacy (WEP) key to be programmed with the **security wep-key** command. Use the **no** form of this command to return to the default setting. Variations of this command include:

security wep-key-length 104
security wep-key-length 128
security wep-key-length 40

The addition of 24-bit initialization vector (IV) makes the 40 bits become 64 bits, 104 bits become 128, and 128 bits become 152 on the client.

Syntax Description

wep-key-length	Specifies the WEP key length. Valid entries are **40**, **104**, and **128**.

Default Values

By default, no keys are defined.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Functional Notes

There are four keys to program. At least one WEP key must be defined. The corresponding number of hexadecimal characters required is determined by:

key size on client, key size on AP = number of keys multiplied by the hexadecimal characters in the key

Examples:

64, 40 = 4 x 10
128, 104 = 4 x 26
152, 128 = 4 x 32

Usage Examples

The following example sets the WEP key length to **104**:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security wep-key-length 104**

security wep-key seed *<passphrase>*

Use the **security wep-key seed** command to set a passphrase for the generation of wired equivalency privacy (WEP) keys for use in **wep shared-key** and **wep open-key** security modes (refer to the command *security mode on page 3539*). Use the **no** form of this command to clear the passphrase.

Syntax Description

<passphrase>	A phrase of **1** to **32** characters used as the basis for WEP key generation.

Default Values

By default, no passphrase is set.

Command History

Release 17.2	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Functional Notes

The generation of WEP keys occurs through the use of a standard message digest 5 (MD5) key generator. The generator creates secure WEP keys by assigning random values for each element (letters or numbers) in the passphrase. Refer to the command *security wep-key generate on page 3544* for more information.

Usage Examples

The following example creates a passphrase of **Adtran6808** to use in WEP key generation on 802.11bg wireless radio on virtual access point (VAP) 1:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security wep-key seed Adtran6808**

security wpa group-key

Use the **security wpa group-key** command to enable group key (broadcast key) rotation for the specified virtual access point (VAP). Use the **no** form of this command to disable group key rotation. Variations of this command include:

security wpa group-key
security wpa group-key change <*minutes*>
security wpa group-key change <*minutes*> **membership-termination**

Syntax Description

change <*minutes*>	Enables a periodic change of the group key. Specify the number of minutes between group key changes. Valid range is **10** to **600** minutes, with the default being **30** minutes.
membership-termination	Optional. Specifies a change of the group key at the termination of any membership association.

Default Values

By default, group key rotation is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example enables wired WPA group key rotation on the VAP:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security wpa group-key**

The following example enables a **15**-minute change of the group key and also enables the group key to change any time a membership is terminated:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security wpa group-key change 15 membership-termination**

ssid

Use the **ssid** command to assign the service set identifier (SSID) for this virtual access point (VAP) and indicate whether to broadcast the SSID over the network. The SSID is a unique identifier consisting of up to 32 characters (letters or numbers). Use the **no** form of this command to return to the default setting. Variations of this command include:

ssid broadcast-mode <*text*>
ssid non broadcast-mode <*text*>

Syntax Description

broadcast-mode	Enables broadcasting the SSID in beacons transmitted for this VAP.
non broadcast-mode	Blocks broadcasting the SSID for this VAP. This setting is used in closed wireless networks. Devices connecting to the access point (AP) in nonbroadcast mode require the wireless device to enter the SSID.
<*text*>	Specifies an SSID for the VAP. The SSID can consist of up to 32 characters using text or letters and can also include spaces.

Default Values

By default, the SSID is set as the concatenation of the string “Adtran”: the **radio-index.vap-index**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example configures the SSID of VAP interface **1** as **WLAN1** and blocks broadcasting this SSID:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#ssid non broadcast-mode WLAN1**

vlan-id *<vlan id>*

Use the **vlan-id** command to associate a virtual local area network (VLAN) with the virtual access point (VAP) interface. Encapsulation 802.1q must be enabled on the access point (AP) before wireless traffic is routed with the VLAN ID attached. To enable encapsulation, refer to the command *encapsulation 802.1q on page 3500*. Use the **no** form of this command to remove an entry.

Syntax Description

<vlan id>	Specifies a VLAN interface ID number. Range is **1** to **4095**.

Default Values

By default, the VLAN ID is the same number as the VAP interface number.

Functional Notes

Once encapsulation 802.1q is enabled on the AP, all wireless traffic received on the VAP's service set identifier (SSID) is mapped to the VLAN (specified by the VLAN ID) when sent out the AP's Ethernet interface. All wireless traffic received on this VLAN ID at the AP's Ethernet interface is mapped to this VAP's SSID for wireless transmission.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example configures the **vlan-id** to **4** for VAP interface **1**:

```
(config)#interface dot11ap 1/1.1
(config-dot11ap 1/1.1-bg)#vlan-id 4
```


NETVANTA 160 SERIES AP INTERFACE COMMAND SET

The NetVanta 160 Series Access Point Interface Configuration command set is used to configure wireless access points (APs) connecting to an AOS platform running the Adtran Wireless Control Protocol (AWCP). The AP is either a physical standalone unit (such as the NetVanta 160 Series) or integrated within an AOS platform via a module, also known as an embedded access point module (EAPM).

Enter the **interface dot11ap** *<ap | ap/radio | ap/radio.vap>* **ap-type nv16x** command at the Global Configuration mode prompt to activate the NetVanta 160 Series AP Interface Configuration mode. For example:

```
>enable
#configure terminal
(config)#interface dot11ap 1 ap-type nv16x
(config-dot11ap 1)#
```

Additional steps must be performed before the NetVanta 160 Series AP is ready for connectivity. The radio-level settings are configured using the NetVanta 160 Series Radio Interface Command Set on page 3567. The virtual access point (VAP) settings are configured using the NetVanta 160 Series VAP Interface Command Set on page 3585.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

access-point controller-standby

Use the **access-point controller-standby** command to release wireless access controller (AC) control of the NetVanta 160 Series wireless access point (AP). This command will cause the AC to stop responding to echo requests from the AP, releasing control of the AP. Use the **no** form of this command to disable this feature.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

No subcommands.

Default Values

By default, controller-standby mode is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example enables controller-standby mode for this AP interface:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#access-point controller-standby**

access-point mac-address *<mac address>*

Use the **access-point mac-address** command to specify the medium access control (MAC) address of the NetVanta 160 Series wireless access point (AP) physical Ethernet interface. Use the **no** form of this command to delete the MAC address of the AP.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Functional Notes

This command binds the wireless access controller (AC) to the AP. Without specifying the MAC address, the AC cannot control the AP.

Usage Examples

The following example configures an AP MAC address of **00:0A:C8:5F:00:D2**:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#access-point mac-address 00:0A:C8:5F:00:D2**

association access-list <*name*>

Use the **association access-list** command to specify a medium access control (MAC) address filter. This filter will only allow specific wireless clients access to the wireless network. A MAC access control list (ACL) must be created before it can be associated with this NetVanta 160 Series wireless access point (AP). Refer to *mac access-list standard <name> on page 1606* for more information. Use the **no** form of this command to remove an associated MAC ACL from this AP.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command dot11ap apply-changes on page 483.

Syntax Description

<name>	Specifies the name of the previously created MAC ACL.

Default Values

By default, no MAC ACLs are associated with an AP.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example configures the AP to use the MAC ACL named **ALLOWLIST** as a filter for allowing access:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#association access-list ALLOWLIST**

country-region

Use the **country-region** command to specify the country region or domain where the NetVanta 160 Series wireless access point (AP) is being used so that the radio can modify its settings to conform to that country's regulations. Use the **no** form of this command to return to the default value. Variations of this command include:

country-region Australia
country-region Austria
country-region Belgium
country-region Bulgaria
country-region Canada
country-region Cyprus
country-region Czech_Republic
country-region Denmark
country-region Estonia
country-region Finland
country-region France
country-region Germany
country-region Greece
country-region Hungary
country-region Iceland
country-region Ireland
country-region Italy
country-region Latvia
country-region Lithuania
country-region Luxembourg
country-region Malta
country-region Mexico
country-region Netherlands
country-region Norway
country-region Poland
country-region Portugal
country-region Puerto_Rico
country-region Romania
country-region Singapore
country-region Slovak_Republic
country-region Slovenia
country-region Spain
country-region Sweden
country-region UK
country-region USA

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

Australia	Specifies Australia configuration.
Austria	Specifies Austria configuration.
Belgium	Specifies Belgium configuration.
Bulgaria	Specifies Bulgaria configuration.
Canada	Specifies Canada configuration.
Cyprus	Specifies Cyprus configuration.
Czech_Republic	Specifies Czech Republic configuration.
Denmark	Specifies Denmark configuration.
Estonia	Specifies Estonia configuration.
Finland	Specifies Finland configuration.
France	Specifies France configuration.
Germany	Specifies Germany configuration.
Greece	Specifies Greece configuration.
Hungary	Specifies Hungary configuration.
Iceland	Specifies Iceland configuration.
Ireland	Specifies Ireland configuration.
Italy	Specifies Italy configuration.
Latvia	Specifies Latvia configuration.
Lithuania	Specifies Lithuania configuration.
Luxembourg	Specifies Luxembourg configuration.
Malta	Specifies Malta configuration.
Mexico	Specifies Mexico configuration.
Netherlands	Specifies Netherlands configuration.
Norway	Specifies Norway configuration.
Poland	Specifies Poland configuration.
Portugal	Specifies Portugal configuration.
Puerto_Rico	Specifies Puerto Rico configuration.
Romania	Specifies Romania configuration.
Singapore	Specifies Singapore configuration.
Slovak_Republic	Specifies Slovak Republic configuration.
Slovenia	Specifies Slovenia configuration.
Spain	Specifies Spain configuration.
Sweden	Specifies Sweden configuration.
UK	Specifies UK configuration.
USA	Specifies USA configuration.

Default Values

By default, the country-region is set to **USA**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP and expanded to include additional country regions.
Release R11.6.0	Command was changed to remove the **uncertified** parameter from the Puerto Rico country region.

Usage Examples

The following example sets the country of operation to **Norway**:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#country-region Norway**

encapsulation 802.1q

Use the **encapsulation 802.1q** command to set the NetVanta 160 Series wireless access point (AP) for virtual local area network (VLAN) encapsulation 802.1q mode. This will apply VLAN tags to the user traffic. Use the **no** form of this command to disable VLAN encapsulation. Variations of this command include:

encapsulation 802.1q
encapsulation 802.1q awcp-vlan <*vlan id*> **native**
encapsulation 802.1q awcp-vlan <*vlan id*> **native priority** <*level*>

> *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

awcp-vlan <*vlan id*>	Optional. Specifies an existing VLAN to be used for Adtran Wireless Control Protocol (AWCP) connection. Valid range is **1** to **4095**. For more information on creating a VLAN, refer to *VLAN Interface Command Set on page 3370*.
native	Enables native mode for the specified VLAN. Packets from this VLAN leaving the interface will not be tagged with the VLAN number. Any untagged packets received by the interface are considered a part of the native VLAN ID. Only one VLAN may be set to **native**. To change where the native VLAN resides, the current native must be disabled using the **no** form of this command before a new one is set.
priority <*level*>	Optional. Specifies the 802.1q priority level for AWCP packets generated by this AP when VLAN tags are applied. Valid range is **1** to **7**, with 1 being the highest priority.

Default Values

By default, **encapsulation 802.1q** is disabled on the AP.

Command History

Release 6.1	Command was introduced.
Release 15.1	Command was added to the NetVanta 150 AP.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Functional Notes

Settings (including encapsulation, VLAN, and native VLAN) for the AP's Ethernet interface must be coordinated with the physical interface to which the AP is connected.

Since all functions on an AP use the same Ethernet interface, there should be only one VLAN ID set to **native** on the entire AP. It is possible that a VLAN can be used on a virtual access point (VAP) and for the AWCP protocol on the AP's Ethernet, but this is not typical. Typically, the control protocol will use the native VLAN and the VAP's data will all be tagged on the Ethernet.

This means that one VLAN on one radio's VAP may be set to **native** or the control protocol (AWCP) VLAN may be set to **native**, but not both unless they both use the same VLAN ID. Typically, the control protocol will use the native VLAN.

If the control protocol and a VAP share the same VLAN ID, control protocol packets will be intercepted by the AP while noncontrol protocol packets will be forwarded to the VAP.

If the AP is to be in trunk mode and the AWCP VLAN is not the native VLAN for the trunk, care must be exercised in transitioning the AP and switchport from access port (nontrunk) mode. The AP should be configured first, then the switchport set to match. When transitioning the AP, set its AWCP VLAN first, then enable trunking mode (encapsulation 802.1q). If the AWCP VLAN is the native VLAN on the AP and switch, AWCP communication will not be lost no matter what combination of trunk mode settings is applied.

Usage Examples

The following example enables encapsulation 802.1q on this AP and makes VLAN 1 the native VLAN:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#encapsulation 802.1q awcp-vlan 1 native**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address for the NetVanta 160 Series access point (AP) Ethernet interface. Use the **no** form of this command to remove a configured IPv4 address.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Functional Notes

The IPv4 address and subnet mask are only needed on the AP interface if the user wants to use remote authentication dial-in user service (RADIUS) authentication with the wireless clients. A default gateway may also need to be specified.

Usage Examples

The following example configures an IPv4 address of **192.22.72.101** and a subnet mask of **255.255.255.252**:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#ip address 192.22.72.101 255.255.255.252**

ip default-gateway *<ipv4 address>*

Use the **ip default-gateway** command to assign a default gateway to the NetVanta 160 Series wireless access point (AP). This allows the AP to communicate with Internet Protocol version 4 (IPv4) devices on other IPv4 subnets. Use the **no** form of this command to remove the default gateway.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<ipv4 address>	Specifies the default gateway IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there is no configured default gateway.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example assigns the AP a default gateway for **10.10.10.1**:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#ip default-gateway 10.10.10.1**

location *<name>*

Use the **location** command to specify the location of the NetVanta 160 Series wireless access point (AP). Use the **no** form of this command to remove the specified location.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<name>	Specifies the name of the location of the AP. The location name may be up to 32 characters.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example assigns the name **FLOOR5** as the location of AP 1:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#location FLOOR5**

logging forwarding on

Use the **logging forwarding on** command to enable the event forwarding feature for the NetVanta 160 Series wireless access point (AP). Use the command *logging forwarding priority-level on page 3563* to specify the event matching the criteria used by AOS to determine whether a message should be forwarded to the remote receiver. Use the **no** form of this command to disable the event forwarding feature.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command dot11ap apply-changes on page 483.

Syntax Description

No subcommands.

Default Values

By default, event notification is disabled on the AP.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables the AOS event forwarding feature for this AP:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#logging forwarding on**

logging forwarding priority-level

Use the **logging forwarding priority-level** command to set the minimum priority threshold for NetVanta 160 Series wireless access point (AP) events sent to the configured remote receiver specified using the command *logging forwarding receiver-ip <ipv4 address> on page 3565*. All events with the specified priority or higher will be sent to all configured remote receivers. Use the **no** form of this command to return to the default priority. Variations of this command include:

logging forwarding priority-level alert
logging forwarding priority-level critical
logging forwarding priority-level debug
logging forwarding priority-level error
logging forwarding priority-level informational
logging forwarding priority-level notice
logging forwarding priority-level warning

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command dot11ap apply-changes on page 483.

Syntax Description

alert	Logs events with **alert** priority (severity level 1, most severe).
critical	Logs events with **critical** priority (severity level 2).
debug	Logs informational events (severity level 7, least severe).
error	Logs events with **error** priority (severity level 3).
informational	Logs **informational** events (severity level 6).
notice	Logs events with **notice** priority (severity level 5).
warning	Logs events with **warning** priority (severity level 4).

Default Values

By default, the **logging forwarding priority-level** is set to **warning**.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example sends all messages with **critical** level or greater to the remote receiver listed using the command *logging forwarding receiver-ip <ipv4 address> on page 3565*:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#logging forwarding priority-level critical**

logging forwarding receiver-ip *<ipv4 address>*

Use the **logging forwarding receiver-ip** command to specify the Internet Protocol version 4 (IPv4) address of the remote receiver server to use when logging NetVanta 160 Series wireless access point (AP) events that match the criteria configured using the command *logging forwarding priority-level on page 3563* command. Use the **no** form of this command to remove a configured address.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command dot11ap apply-changes on page 483.*

Syntax Description

<ipv4 address>	Specifies the IPv4 address of the remote receiver to use when logging messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there are no configured syslog server addresses.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example specifies a remote receiver with address **172.5.67.99** to use when logging AP messages:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#logging forwarding receiver-ip 172.5.67.99**

name <*name*>

Use the **name** command to specify a name for this NetVanta 160 Series wireless access point (AP). Use the **no** form of this command to remove the assigned name.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<name>	Specifies the name of the AP. The name may be up to 32 characters in length.

Default Values

By default, the name of the AP will be ADTN plus the last three bytes of the AP medium access control (MAC) address (all uppercase).

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series AP.

Usage Examples

The following example assigns the name **ACCOUNTING1** to AP 1:

(config)**#interface dot11ap 1 ap-type nv16x**
(config-dot11ap 1)**#name ACCOUNTING1**

NETVANTA 160 SERIES RADIO INTERFACE COMMAND SET

A radio interface is a virtual interface that can be programmed into an AOS platform running the Adtran Wireless Control Protocol (AWCP). This interface is used to configure radio-level commands for an 802.11 wireless access point (AP). The AP is either a physical standalone unit (such as the NetVanta 160 Series) or integrated within the AOS platform via a module, also known as an embedded access point module (EAPM).

The associated AP interface must be configured before access to the Radio Interface Configuration mode is possible. For more information on configuring the AP, refer to *NetVanta 150 AP Interface Command Set on page 3494*. Upon creation, each radio will have one default virtual access point (VAP) configured. More detailed information on configuring the VAP interface is provided in *NetVanta 150 VAP Interface Command Set on page 3533*.

There are only two radio types: 802.11a/n and 802.11b/g/n. Radio 802.11b/g/n defaults to **interface dot11ap** <*ap/***1**> and radio 802.11a/n defaults to **interface dot11ap** <*ap/***2**>. The only changes that can be made to the radio types is to specify the radio mode of the 802.11b/g/n radio as type b/g, b/g/n, or g/n, or the radio mode of the 802.11a/n radio as type a or a/n using the command *radio-mode on page 3579*.

The parent (AP) interface must be created before access to the NetVanta 160 Radio Interface Configuration mode is possible. Execute the command ***interface dot11ap*** *<ap>* ***ap-type nv16x*** *command to create an AP interface.*

To activate NetVanta 160 Radio Interface Configuration mode for an 802.11b/g, 802.11b/g/n, or 802.11g/n radio, enter the commands at the Global Configuration mode prompt as shown below:

```
>enable
#configure terminal
(config)#interface dot11ap 1/1
(config-dot11ap 1/1-bg)#
```

To activate Radio Interface Configuration mode for an 802.11a or 802.11a/n radio, enter the commands at the Global Configuration mode prompt as shown below:

```
>enable
#configure terminal
(config)#interface dot11ap 1/2
(config-dot11ap 1/2-a)#
```

By default, ***interface dot11ap*** *<ap/***1***> is radio type 802.11b/g/n and* ***interface dot11ap*** *<ap/***2***> is radio type 802.11a/n.*

*Not all radio interface commands apply to both radio types.Use the **?** command to display a list of valid commands.*

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

antenna on page 3569
beacon period <time> on page 3570
channel <number> on page 3571
channel-width-40MHz on page 3573
dtim-interval <number> on page 3574
fragment-threshold <length> on page 3575
inactivity-timeout max <value> on page 3576
packet-aggregation on page 3577
power local on page 3578
radio-mode on page 3579
rts threshold <length> on page 3580
secondary-channel <number> on page 3581
speed on page 3583
world-mode dot11d on page 3584

antenna

Use the **antenna** command to select the desired antenna mode. Use the **no** form of this command to return to the default value. Variations of this command include the following:

antenna mimo-1x1
antenna mimo-2x2

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

mimo-1x1	Sets the antenna mode to transmit or receive on antenna 1.
mimo-2x2	Sets the antenna mode to transmit or receive on antenna 2.

Default Values

By default, the antenna is set to **mimo-2x2**.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example sets the antenna mode to transmit or receive on antenna 1 on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#antenna mimo-1x1**

beacon period *<time>*

Use the **beacon period** command to set the time between beacons. Use the **no** form of this command to return to the default value.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<time>	Specifies the number of 802.11 time units (TUs) between beacons. One TU is 1024 microseconds. Range is **20** to **1000** TU.

Default Values

By default, the beacon period is **100** TU.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

A beacon is a type of management frame used in 802.11 wireless networks. Beacon frames carry important information, such as the basic service set, parameter sets, and capability. The beacon frame is sent to the broadcast medium access control (MAC) address, which means that all clients must be able to receive and process beacons.

Beacon frames are associated with some overhead, which decreases the throughput of the wireless network. The higher the beacon period, the fewer number of beacons sent, thus reducing overhead and increasing throughput on the network. However, fewer beacons can cause a delay in the association process because stations scanning for available access points (APs) may miss the beacons.

Usage Examples

The following example sets the beacon period to **500** TU on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#beacon period 500**

channel *<number>*

Use the **channel** command to manually select a channel for the wireless radio. Use the **no** form of this command to return to the default value.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point (AP), you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<number>	Specifies the Institute of Electrical and Electronics Engineers, Inc. (IEEE) channel number. The range of channels is dependent on the radio type and country setting.

Default Values

By default, the channel number is automatically set to a channel corresponding to the AP number. The available channels depend on the radio type. For example, if there are three APs configured on a 2.4 Ghz radio, channels 1, 6, and 11 can be used. The first AP defaults to channel 1, the second AP defaults to channel 6, and the third AP defaults to channel 11. The available channels are different for a 5 Ghz radio.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.
Release R11.7.0	Command was altered to remove the **least-congested** parameter.

Functional Notes

The available channel range varies by the radio type and country setting specified on the NetVanta 160 Series AP. For more information about specific channels available to each radio type for a specific country, refer to the configuration guide *NetVanta 160 Series Wireless Configuration Guide*, available online at https://supportcommunity.adtran.com.

> NOTE *Type **channel ?** to display a list of valid channels from which to choose. The list of channels displayed is based on the selected radio type (refer to the command* *radio-mode on page 3579**) and country setting (refer to the command* *country-region on page 3498**).*

Usage Examples

The following example manually sets an 802.11b/g/n wireless radio to channel **6** in the United States:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#channel 6**

The following example manually sets an 802.11a/n wireless radio to channel **149** in the United States:

(config)**#interface dot11ap 1/2 radio-type 802.11a**
(config-dot11ap 1/1-a)**#channel 149**

channel-width-40MHz

Use the **channel-width-40MHz** command to enable the 40 MHz mode of the radio. Use the **no** form of this command to disable the radio's 40 MHz mode.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

No subcommands.

Default Values

By default, the 40 MHz radio mode is disabled.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

This feature is only available on an 802.11n radio, such as the 802.11b/g/n, 802.11g/n, or 802.11a/n radios. Refer to the command *radio-mode on page 3579* for information about changing the AP's radio mode.

Usage Examples

The following example enables the 40 MHz channel width on the 802.11a/n radio:

(config)**#interface dot11ap 1/2 radio-type 802.11a**
(config-dot11ap 1/1-an)**#channel-width-40MHz**

dtim-interval <*number*>

Use the **dtim-interval** command to specify the delivery traffic indication message (DTIM) interval period on the radio. The DTIM interval period is a number of beacon intervals at which the radio sends buffered multicast and broadcast frames. This feature helps radios operating in power-saving mode. Use the **no** form of this command to return the DTIM interval to the default value.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

<*number*>	Specifies the number of DTIM beacon intervals. Valid range is **1** to **255**.

Default Values

By default, the DTIM interval is **1**.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

This feature is only available on an 802.11n radio, such as the 802.11b/g/n, 802.11g/n, or 802.11a/n radios. Refer to the command *radio-mode on page 3579* for information about changing the AP's radio mode.

Usage Example

The following example changes the DTIM interval to **10** on the 802.11 b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type bg**
(config-dot11ap 1/1-bg)**#dtim-interval 10**

fragment-threshold *<length>*

Use the **fragment-threshold** command to set the packet length threshold. Packets larger than the value set in this command will be fragmented when transmitted on the wireless link. Use the **no** form of this command to return to the default value.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<length>	Specifies the maximum packet length allowed before fragmentation will occur. Range is **256** to **2346** bytes.

Default Values

By default, the fragment threshold is set at **2346** bytes.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

The fragment threshold can be set to a lower number to prevent retransmission of large packets, but the overhead will increase. If the threshold is large, the overhead is relatively small but large packets will be retransmitted, lowering efficiency.

Usage Examples

The following example sets the fragment threshold at **572** bytes on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#fragment-threshold 572**

inactivity-timeout max *<value>*

Use the **inactivity-timeout max** command to set the maximum length of inactivity allowed between an access point (AP) and its clients. If no response is seen from the client within the timeout period, the client will be disassociated. Use the **no** form of this command to return to the default value.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

<value>	Specifies the maximum length of time a connection between an AP and a client is allowed to remain inactive. Range is **1** to **99** minutes.

Default Values

By default, the maximum inactivity timeout is **5** minutes.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Usage Examples

The following example sets the maximum inactivity timeout to **2** minutes on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#inactivity-timeout max 2**

packet-aggregation

Use the **packet-aggregation** command to enable packet aggregation for 802.11n clients. Use the **no** form of this command to disable packet aggregation.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

No subcommands.

Default Values

By default, packet aggregation is enabled.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

This feature is only available on an 802.11n radio, such as the 802.11b/g/n, 802.11g/n, or 802.11a/n radios. Refer to the command *radio-mode on page 3579* for information about changing the AP's radio mode.

Usage Examples

The following example disables packet-aggregation for the 802.11n clients on the 802.11b/g/n radio:

(config)**#interface dot11ap 1/1 radio-type bg**
(config-dot11ap 1/1-bg)**#no packet-aggregation**

power local

Use the **power local** command to select the radio's transmit power level. The range of the power level is relative to the country region currently specified for the radio. Use the **no** form of this command to return to the default value. Variations of this command include:

power local eighth
power local half
power local maximum
power local minimum
power local quarter

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

eighth	Sets the power local level to one-eighth of the maximum output power setting.
half	Sets the power local level to one-half of the maximum output power setting.
maximum	Sets the power local level to the maximum output power setting.
minimum	Sets the power local level to the minimum output power setting.
quarter	Sets the power local level to one-fourth of the maximum output power setting.

Default Values

By default, the power local setting is **maximum**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

Radio cell size and interference between cells can be reduced by lowering the radio's transmit power level.

Usage Examples

The following example sets the radio's transmit power to one-half maximum power on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#power local half**

radio-mode

Use the **radio-mode** command to set the radio to use a specific 802.11 protocol. Use the **no** form of this command to return to the default value. Variations of this command include the following:

radio-mode a
radio-mode an
radio-mode bg
radio-mode bgn
radio-mode gn

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

a	Specifies the radio operates using 802.11a.
an	Specifies the radio operates using 802.11a/n.
bg	Specifies the radio operates using 802.11b/g.
bgn	Specifies the radio operates using 802.11b/g/n.
gn	Specifies the radio operates using 802.11g/n.

Default Values

By default, the 802.11bg radio is set to **radio-mode bgn** and the 802.11a radio is set to **radio-mode an**.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

Adtran currently supports these IEEE 802.11 wireless local area network (WLAN) standards: 802.11a, 802.11b, 802.11g, and 802.11n. Each access point (AP) contains two integrated radios: one that supports 802.11a and 802.11n, and one that supports 802.11b/g, and 802.11n.

Usage Examples

The following example sets the radio mode to radio type **gn** on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#radio-mode gn**

rts threshold *<length>*

Use the **rts threshold** command to set the threshold for use of request to send (RTS) frames. RTS is used to gain access to the radio frequency (RF) medium when long frames need to be transmitted. The RTS threshold defines the minimum long frame length that will require RTS/clear to send (CTS) prior to transmission. Any frame that matches or is longer than the length specified in the **rts threshold** command must be preceded by a RTS/CTS on the RF medium. Use the **no** form of this command to return to the default value.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

<length>	Specifies the length of the RTS threshold in bytes. Range is **256** to **2346** bytes.

Default Values

By default, the RTS threshold is **2346** bytes.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Functional Notes

Generally, it is best to set the RTS threshold as high as possible. However, the threshold may need to be set lower if network throughput is sluggish or there are a high number of frame retransmissions.

Usage Examples

The following example sets the RTS threshold to **1024** bytes on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#rts threshold 1024**

secondary-channel *<number>*

Use the **secondary-channel** command to set the 802.11n secondary operating channel when the radio is operating in the 40 MHz mode (refer to the command *channel-width-40MHz on page 3573*). Any valid channel, other than the primary channel set with the command *channel <number> on page 3571* can be used. Use the **no** form of this command to remove the secondary channel.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point (AP), you must apply those changes for them to take effect using the command dot11ap apply-changes on page 483.*

Syntax Description

<number>	Specifies the secondary channel. Any valid channel, other than the primary channel, is accepted. Valid range is **1** to **13**, depending on the country setting of the radio.

Default Values

By default, the secondary 802.11n channel is set to **0**.

Command History

Release R10.4.0	Command was introduced.
Release R11.7.0	Command was altered to remove the **auto** parameter.

Functional Notes

The secondary channels available depend on the primary channel selected and the country. The secondary channels available are either four channels above, or four channels below the selected primary channel. The following table describes the available secondary channels based on the primary channel.

Primary Channel	Upper Secondary Channel	Lower Secondary Channel
1	5	N/A
2	6	N/A
3	7	N/A
4	8	N/A
5	9	1
6	10	2
7	11	3
8	12	4

Primary Channel	Upper Secondary Channel	Lower Secondary Channel
9	13	5
10	N/A	6
11	N/A	7
12	N/A	8
13	N/A	9

For more information about specific channels available to each radio type for a specific country, refer to the configuration guide *NetVanta 160 Series Wireless Configuration Guide*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the secondary 802.11n channel for the b/g/n radio is set to **1**:

(config)**#interface dot11ap 1/1 radio-type bg**
(config-dot11ap 1/1-bg)**#secondary-channel 1**

speed

Use the **speed** command to set the active rate for the radio. Frames cannot be transmitted at a speed that is higher than the specified active rates. Use the **no** form of this command to return to the default value. Variations of this command include the following:

speed best
speed <*speed*>

> *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

best	Sets the transmit speed of the radio to the best available.
<*speed*>	Sets the transmit speed of the radio. Available speeds vary based on the setting in the **radio-mode** command. Choose from 6, 9, 12, 18, 24, 36, 48, or 54 Mbps for a b/g/n radio, or 6, 9, 12, 18, 24, 36, 48, or 54 Mbps for an a/n radio.

> *The **speed** setting **best** is recommended.*

Default Values

By default, the active rate is set to **best**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Usage Examples

The following example sets the active rate to **54** Mbps on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#speed best**

world-mode dot11d

Use the **world-mode dot11d** command to enable 802.11d mode. This mode allows country codes to be transmitted in beacons sent from the access point (AP). Use the **no** form of this command to disable 802.11d mode.

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

No subcommands.

Default Values

By default, **802.11d** mode is enabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series radio interface.

Usage Examples

The following example enables 802.11d mode on an 802.11b/g/n wireless radio:

(config)**#interface dot11ap 1/1 radio-type 802.11bg**
(config-dot11ap 1/1-bg)**#world-mode dot11d**

NETVANTA 160 SERIES VAP INTERFACE COMMAND SET

The NetVanta 160 Virtual Access Point (VAP) Interface Configuration command set is used to configure service set identifiers (SSIDs) security and other parameters for each VAP.

A VAP is a logical entity that can exist within a physical wireless access point (AP). VAPs are virtual interfaces represented on wireless networks through the use of a wireless access controller (AC) running the Adtran Wireless Control Protocol (AWCP) and an AP. Each physical AP can support up to eight VAPs for each of the two radio bands for a total of 16 VAPs. VAPs are distinguished by an SSID and can be mapped to a virtual local area network (VLAN). VLAN information can be shared across switches with Ethernet trunks. A common configuration has two VAPs, one associated to a corporate VLAN, and one associated to a guest VLAN.

The associated AP and radio interfaces must be configured before attempting to configure the VAP. For more information on configuring the AP and radios, refer to *NetVanta 160 Series AP Interface Command Set on page 3550* and *NetVanta 160 Series Radio Interface Command Set on page 3567*. Each radio will have one default VAP already configured. The VAP name is based on the interface to which the AP and radio are mapped using the following syntax, **interface dot11ap** *<ap/radio.vap>*.

To add a VAP or to enter its interface configuration mode, enter the **interface dot11ap** *<ap/radio.vap>* command identifying the appropriate AP and radio interface, followed by the VAP interface number. This command can be entered from the Global Configuration mode prompt or from any other interface configuration mode prompt. In the following example, VAP 1 is created for AP 1 with an 802.11b/g/n radio. For example:

```
>enable
#configure terminal
(config)#interface dot11ap 1/1.1
(config-dot11ap 1/1.1-bg)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

accounting on page 3587
client-separation on page 3589
radius-server host on page 3590
security mode on page 3592

security wpa group-key on page 3594
ssid on page 3595
vlan-id <vlan id> on page 3596

accounting

Use the **accounting** command to enable remote authentication dial-in user service (RADIUS) accounting for associations with this virtual access point (VAP) and specify update intervals. Use the **no** form of this command to disable accounting for this VAP. Variations of this command include:

accounting enabled
accounting update
accounting update newinfo
accounting update periodic
accounting update periodic <*value*>

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command dot11ap apply-changes on page 483.*

Syntax Description

enabled	Enables RADIUS accounting on this VAP.
update	Defines the RADIUS accounting update setting. Executing the **accounting update** command without specifying any further parameters will send updates when new information occurs. This is the same as executing the **accounting update newinfo** command.
newinfo	Specifies sending RADIUS accounting records as they occur.
periodic	Specifies collecting accounting records and sending them periodically. The default value is **5**.
<*value*>	Optional. Specifies the number of minutes between periodic accounting updates. Valid range is **1** to **99**.

Default Values

By default, RADIUS accounting is disabled.

Functional Notes

The RADIUS server host, access point (AP) IP address, and IP gateway must be configured on the access point for this feature to function. Refer to *radius-server host on page 3590*, *ip address <ipv4 address> <subnet mask> on page 3559*, and *ip default-gateway <ipv4 address> on page 3560* for more information on configuring these parameters.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example enables RADIUS accounting for associations with this VAP:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#accounting enabled**

The following example enables sending RADIUS accounting updates as they occur for this VAP:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#accounting update newinfo**

client-separation

Use the **client-separation** command to prevent wireless clients within this virtual access point (VAP) from communicating directly with each other. Use the **no** form of this command to disable this feature, allowing clients to communicate with one another. It is recommended to enable this command.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example prevents wireless clients on this VAP interface from communicating directly with each other:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#client-separation**

radius-server host

Use the **radius-server host** command to specify the parameters for a remote authentication dial-in user service (RADIUS) server to be used when sending RADIUS messages from the virtual access point (VAP). At a minimum, the Internet Protocol version 4 (IPv4) address of the server must be given. The other parameters are also allowed and (if not specified) will use default values or fall back on the global RADIUS server's default settings. Use the **no** form of this command to remove the RADIUS server properties and prevent the VAP from using authentication, authorization, and accounting (AAA) methods. Variations of this command include:

radius-server host *<ipv4 address>* **acct-port** *<port>* **auth-port** *<port>* **key** *<key>*
radius-server host *<ipv4 address>* **acct-port** *<port>* **key** *<key>*
radius-server host *<ipv4 address>* **auth-port** *<port>* **acct-port** *<port>* **key** *<key>*
radius-server host *<ipv4 address>* **auth-port** *<port>* **key** *<key>*
radius-server host *<ipv4 address>* **key** *<key>*

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address for the RADIUS server. IPv4 address should be expressed in dotted decimal notation (for example, **10.10.10.1**).
acct-port	Specifies the remote port to which to send accounting requests.
auth-port	Specifies a remote port to which to send authentication requests.
<port>	Specifies a User Datagram Protocol (UDP) port number to be used when sending authentication or accounting information to the RADIUS server. Valid range is **1** to **65535**.
key *<key>*	Defines the shared key used between the RADIUS server and the access point. The key must appear last on the input line since it reads the rest of the line beyond the **key** keyword. The maximum length is 64 bytes.

Default Values

By default, a RADIUS server is not defined. The default setting for **acct-port** is **1813** and for **auth-port** is **1812**. By default, no **key** is configured. The IPv4 address in this command refers to the default virtual routing and forwarding (VRF) instance only.

Command History

Release 15.1	Command was expanded to include the VAP interface.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example defines the RADIUS server parameters with an IPv4 address of **10.10.10.1**, sets the accounting port to **1646**, and configures the shared key as **ABC123**:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#radius-server host 10.10.10.1 acct-port 1646 key ABC123**

security mode

Use the **security mode** command to configure the security mode settings for this virtual access point (VAP). Use the **no** form of this command to return to the default setting. Depending on the mode chosen none and wi-fi protected access (WPA), further command options are available. Variations of this command include:

security mode none
security mode wpa aes-ccmp eap
security mode wpa aes-ccmp psk <*key*>
security mode wpa aes-ccmp tkip eap
security mode wpa aes-ccmp tkip psk <*key*>
security mode wpa tkip aes-ccmp eap
security mode wpa tkip aes-ccmp psk <*key*>
security mode wpa tkip eap
security mode wpa tkip psk <*key*>

In order to connect to the access point (AP), a client must support the same security mode as configured on this VAP.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

none	Specifies that no security be used on this VAP. There is no authentication required to connect to this VAP and no encryption is provided on the wireless connection.
wpa	Configures this VAP for WPA security mode.
aes-ccmp	Specifies using the WPA2 algorithms. This security setting can be used alone or in combination with Temporal Key Integrity Protocol (TKIP).
eap	Specifies that the WPA security mode use the Extensible Authentication Protocol (EAP) as a universal authentication framework in the wireless network. Authentication is performed between the client and a remote authentication dial-in user service (RADIUS) server.
psk	Specifies that the WPA security mode use preshared keys (PSKs) for key management. PSK may be used in combination with **tkip** and/or **aes-ccmp**. This method does not require a RADIUS authentication server. The PSK must be known on all VAP clients.
<*key*>	Defines the PSK for security. The key must consist of 8 to 63 ASCII or 16 to 126 hexadecimal characters. Clients supporting WPA PSK are allowed to connect to this VAP.

tkip	Specifies that the WPA security mode use TKIP as its keying structure. This protocol specifies the algorithms used for rotating keys. TKIP can be used alone or in combination with **aes-ccmp**.

Default Values

By default, no security mode is defined.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.
Release R11.6.0	Command was changed to remove **wep open-key** and **wep shared-key** security modes.

Usage Examples

The following example shows a typical configuration of these parameters:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security mode wpa tkip psk myPresharedKey**

security wpa group-key

Use the **security wpa group-key** command to enable group key (broadcast key) rotation for the specified virtual access point (VAP). Use the **no** form of this command to disable group key rotation. Variations of this command include:

security wpa group-key
security wpa group-key change <*minutes*>
security wpa group-key change <*minutes*> **membership-termination**

> NOTE *If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command* *dot11ap apply-changes on page 483*.

Syntax Description

change <*minutes*>	Enables a periodic change of the group key. Specify the number of minutes between group key changes. Valid range is **10** to **600** minutes, with the default being **30** minutes.
membership-termination	Optional. Specifies a change of the group key at the termination of any membership association.

Default Values

By default, group key rotation is disabled.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example enables wired WPA group key rotation on the VAP:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security wpa group-key**

The following example enables a **15**-minute change of the group key and also enables the group key to change any time a membership is terminated:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#security wpa group-key change 15 membership-termination**

ssid

Use the **ssid** command to assign the service set identifier (SSID) for this virtual access point (VAP) and indicate whether to broadcast the SSID over the network. The SSID is a unique identifier consisting of up to 32 characters (letters or numbers). Use the **no** form of this command to return to the default setting. Variations of this command include:

ssid broadcast-mode *<text>*
ssid nonbroadcast-mode *<text>*

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

broadcast-mode	Enables broadcasting the SSID in beacons transmitted for this VAP.
nonbroadcast-mode	Blocks broadcasting the SSID for this VAP. This setting is used in closed wireless networks. Devices connecting to the access point (AP) in nonbroadcast mode require the wireless device to enter the SSID.
<text>	Specifies an SSID for the VAP. The SSID can consist of up to 32 characters using text or letters and can also include spaces.

Default Values

By default, the SSID is set as the concatenation of the string “Adtran”: the **radio-index.vap-index**.

Command History

Release 15.1	Command was introduced.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example configures the SSID of VAP interface **1** as **WLAN1** and blocks broadcasting this SSID:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#ssid non broadcast-mode WLAN1**

vlan-id *<vlan id>*

Use the **vlan-id** command to associate a virtual local area network (VLAN) with the virtual access point (VAP) interface. Encapsulation 802.1q must be enabled on the access point (AP) before wireless traffic is routed with the VLAN ID attached. To enable encapsulation, refer to the command *encapsulation 802.1q on page 3557*. Use the **no** form of this command to remove an entry.

If you change any part of the configuration of the NetVanta 160 Series access point, you must apply those changes for them to take effect using the command *dot11ap apply-changes on page 483*.

Syntax Description

<vlan id>	Specifies a VLAN interface ID number. Range is **1** to **4094**.

Default Values

By default, the VLAN ID is the same number as the VAP interface number.

Functional Notes

Once encapsulation 802.1q is enabled on the AP, all wireless traffic received on the VAP's service set identifier (SSID) is mapped to the VLAN (specified by the VLAN ID) when sent out the AP's Ethernet interface. All wireless traffic received on this VLAN ID at the AP's Ethernet interface is mapped to this VAP's SSID for wireless transmission.

Command History

Release 15.1	Command was expanded to include the VAP interface.
Release R10.4.0	Command was added to the NetVanta 160 Series VAP interface.

Usage Examples

The following example configures the **vlan-id** to **4** for VAP interface **1**:

(config)**#interface dot11ap 1/1.1**
(config-dot11ap 1/1.1-bg)**#vlan-id 4**

CARRIER ETHERNET COMMAND SETS

The Carrier Ethernet command sets are divided into the following sections:

EFM NIM2 ETHERNET COMMAND SETS

This section includes the following command sets:

MEF EFM GROUP COMMAND SET

Metro Ethernet Forum (MEF) Ethernet in the first mile (EFM) groups are logical interfaces that represent an EFM bonding group. Interfaces are connected to the EFM group and provide physical links to carry bonded traffic. These groups are used with the EFM network interface modules (NIM2s).

EFM NIM2s are used by Adtran products to provide EFM capabilities across wide area network (WAN) interfaces. These NIM2 cards enable host devices to participate in existing Metro Ethernet networks (MENs) that are deployed with EFM technology. The EFM group operates as the MEN port for the AOS unit, allowing Ethernet virtual connections (EVCs) to be associated logically as a MEN port and to use the same interfaces for connection with the MEN.

EFM groups are created and configured using the **interface efm-group** <*slot/port*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#interface efm-group 1/1
(config-efm-group 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

connect on page 3600
loopback detection on page 3601
thresholds xcv on page 3602
xcv-link-removal on page 3603

connect

Use the **connect** command to specify a physical interface to connect to the Ethernet in the first mile (EFM) group. Use the **no** form of this command to remove the connected interface from the group. Variations of this command include:

connect e1 <*slot/port*>
connect shdsl <*slot/port*>
connect t1 <*slot/port*>

Syntax Description

e1 <*slot/port*>	Specifies that an E1 interface is connected to the group.
shdsl <*slot/port*>	Specifies that a single-pair high-speed digital subscriber line (SHDSL) interface is connected to the group.
t1 <*slot/port*>	Specifies that a T1 interface is connected to the group.

Default Values

By default, no interfaces are connected to the EFM group.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example connects the SHDSL interface **shdsl 1/1** to EFM group **1**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#connect shdsl 1/1**

loopback detection

Use the **loopback detection** command to enable loopback detection on the Ethernet in the first mile (EFM) group. Use the **no** form of this command to disable loopback detection.

Syntax Description

No subcommands.

Default Values

By default, looback detection is enabled.

Command History

Release A5.02	Command was introduced.

Functional Notes

Loopback detection is a function of the EFM engine on the Quad single-pair high-speed digital subscriber line (SHDSL) and Quad T1/E1 EFM network interface modules (NIM2s). When loopback detection is enabled, the EFM engine attaches its media access control (MAC) address to EFM fragments when they leave the module. The EFM engine also inspects EFM framents to verify that the MAC address on the fragments does not match the EFM engine's own MAC address. If the EFM fragment does have the same MAC address as the EFM engine, a loopback detection condition is asserted, and the EFM engine automatically removes the offending link from the EFM group.

Usage Examples

The following example disables loopback detection

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#no loopback detection.**

thresholds xcv

Use the **thresholds xcv** command to configure the excessive code violation threshold for the interface's link in the Ethernet in the first mile (EFM) group. When this threshold is crossed, the link is removed from the group. Use the **no** form of this command to return the threshold to the default value. Variations of this command include:

thresholds xcv 1e-5
thresholds xcv 1e-6
thresholds xcv 1e-7

Syntax Description

1e-5	Specifies that the threshold is set at a 1e-5 bit error rate.
1e-6	Specifies that the threshold is set at a 1e-6 bit error rate.
1e-7	Specifies that the threshold is set at a 1e-7 bit error rate.

Default Values

By default, thresholds are set to **1e-7**.

Command History

Release A3.01	Command was introduced.

Functional Notes

Once the threshold is set, the command *xcv-link-removal on page 3603* must be entered in the group's configuration so that the interface's link is removed when the threshold is crossed.

Usage Examples

The following example specifies that the excessive code violation threshold for interfaces connected to EFM group **1** is **1e-6**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#thresholds xcv 1e-6**

xcv-link-removal

Use the **xcv-link-removal** command to remove an interface's link from the Ethernet in the first mile (EFM) group if the excessive code violation threshold is exceeded. This threshold is set using the command *thresholds xcv on page 3602*. Using the **no** form of this command disables the link removal.

Syntax Description

No subcommands.

Default Values

By default, link removal is enabled for the EFM group.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that an interface whose excessive code violations exceed the threshold is no longer linked to EFM group **1**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#xcv-link-removal**

MEF ETHERNET INTERFACE

The Metropolitan Ethernet Forum (MEF) Ethernet interface is a virtual interface used by AOS products to interface with the Metro Ethernet network (MEN) and carrier Ethernet technologies. The MEF Ethernet interface functions as the user-network interface (UNI) in AOS products with the second-generation Ethernet in the First Mile (EFM) network interface modules (NIMs). The MEF Ethernet interface is used as the Layer 2 and 3 wide-area network (WAN) interface. For more information about configuring the MEF Ethernet interface as part of the EFM NIM2 configuration, refer to the configuration guide *Configuring EFM NIM2s and the MEF Ethernet Interface in AOS* available online at https://supportcommunity.adtran.com.

To activate the basic MEF Ethernet Interface Configuration mode, enter the **interface mef-ethernet** *<slot/port>* command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface mef-ethernet 0/1
(config-mef-ethernet 0/1)#
```

To activate the basic MEF Ethernet Subinterface Configuration mode, enter the **interface mef-ethernet** *<slot/port.subinterface>* command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface mef-ethernet 0/1.1
(config-mef-ethernet 0/1.1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

arp arpa on page 3606
awcp on page 3607
bandwidth <value> on page 3608
crypto map <name> on page 3610
dynamic-dns on page 3612
encapsulation 802.1q on page 3614

arp arpa

Use the **arp arpa** command to set ARPA as the standard Address Resolution Protocol (ARP) on this interface. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

The default for this command is **arpa**.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example enables standard ARP for the MEF Ethernet interface **0/1**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#arp arpa**

awcp

Use the **awcp** command to enable Adtran Wireless Control Protocol (AWCP) on this interface. The AWCP is an Adtran proprietary protocol used by an access controller (AC) to communicate with an access point (AP). Use the **no** form of this command to disable AWCP for this interface.

Syntax Description

No subcommands.

Default Values

By default, AWCP is enabled on the interface.

Command History

Release 15.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

When the global-level command **dot11ap access-point-controller** (refer to *dot11ap access-point-control on page 1268* for more information) is enabled, the AWCP function can be disabled on a specific interface by using the **no** form of this command from the desired interface. When the global-level command **dot11ap access-point-controller** is disabled, it overrides the **awcp** command setting for the interface.

Usage Examples

The following example disables AWCP on the MEF Ethernet interface 0/1:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#no awcp**

bandwidth <*value*>

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default value.

Syntax Description

<*value*>	Specifies bandwidth in kbps. Range is **1** to **4294967295** kbps.

Default Values

To view default value, use the **show interfaces** command.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher level protocols to be used in cost calculations. While this is a routing parameter that does not affect the physical interface, it does affect the amount of bandwidth available for use in Quality of Service (QoS) configurations.

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This can be misleading in QoS configurations if the **bandwidth** command has been applied to the IP interface for routing purposes because the command overrides the reported available bandwidth that can be utilized for QoS. Using the **bandwidth** command can severely disrupt the configuration of QoS on the interface, therefore, use the **max-reserved-bandwidth** command (*page 3660*) to adjust the bandwidth appropriately for QoS configurations.

When configuring QoS for an Ethernet or VLAN interface, the interface **traffic-shape rate** command can be used to configure traffic shaping without applying a QoS map. If traffic shaping is applied to the same interface that will also have a QoS map applied to it, the amount of bandwidth available for the QoS policy is reduced to the value set with the **traffic-shape rate** command (*page 3668*). This value should be set to match the upload speed of the circuit. For example, under normal circumstances, an Ethernet interface can negotiate to 100 Mbps. However, the throughput of the upstream equipment is usually significantly less than the negotiated rate. The **traffic-shape rate** command is used to define the limit of when QoS policies containing the commands *bandwidth on page 4466* or *priority on page 4481* should be enforced according to the upload speed of the circuit. If the **bandwidth** <*value*> command is also entered on the same IP interface as the **traffic-shape rate** command, it will overwrite the value of the **traffic-shape rate** command for QoS purposes. It is not recommended to use the **bandwidth** <*value*> command for QoS. Instead, use the **max-reserved-bandwidth** command (*page 3660*) to adjust the bandwidth appropriately because the **traffic-shape rate** command is required for QoS to function properly on VLAN and Ethernet WAN IP interfaces.

Usage Examples

The following example sets bandwidth of the MEF Ethernet 0/1 interface to 10 Mbps:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#bandwidth 10000**

crypto map *<name>*

Use the **crypto map** command to associate crypto maps with the interface. Use the **no** form of this command to remove a crypto map from an interface.

When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.

Syntax Description

<name>	Specifies the crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

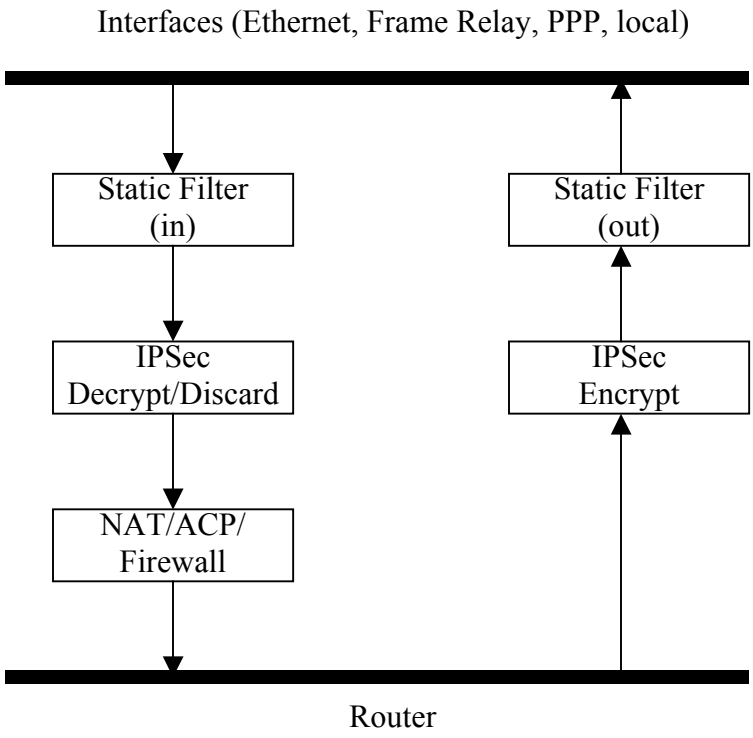
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the policy class and associated access control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#crypto map MyMap**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies the user name.
<*password*>	Specifies the password.
	Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user's name **user**, and password **pass**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#dynamic-dns dyndns-custom host user pass**

encapsulation 802.1q

Use the **encapsulation 802.1q** command to put the interface into 802.1q virtual local area network (VLAN) mode.

If you are using 802.1q encapsulation with the MEF Ethernet interface, you must have a native VLAN MEF Ethernet subinterface configured for the EFM NIM2 to communicate with the AOS unit. Refer to the Functional Notes of this command for more information.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

To use 802.1q encapsulation with the MEF Ethernet interface, you must have a native VLAN MEF Ethernet subinterface configured using the command *vlan-id <vlan id> on page 3669*:

Usage Examples

The following example configures a MEF Ethernet subinterface for VLAN usage and puts the MEF Ethernet interface 0/1 in 802.1q mode:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vlan-id 1 native**
(config-mef-ethernet 0/1.1)**#exit**

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#encapsulation 802.1q**

ethernet-cfm down

Use the **ethernet-cfm down** command to enable Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) on the Ethernet interface. Use the **no** form of this command to disable Ethernet OAM CFM on this interface.

Syntax Description

No subcommands.

Default Values

By default, Ethernet OAM CFM is disabled.

Command History

Release 17.4	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

For more information about Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

For more information regarding specific Ethernet OAM CFM configuration commands on the Ethernet interface, refer to the *Ethernet OAM CFM Command Set on page 4405*.

Usage Examples

The following example enables Ethernet OAM CFM on the MEF Ethernet interface 0/1:

```
(config)#interface mef-ethernet 0/1
(config-mef-ethernet 0/1)#ethernet-cfm down
```


ethernet-cfm mep

Use the **ethernet-cfm mep** command to create an Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance endpoint (MEP) on the Ethernet interface. Use the **no** form of this command to remove the MEP from the interface. Variations of this command include:

ethernet-cfm mep *<name>* *<name>* *<mep id>* **down**
ethernet-cfm mep none *<name>* *<mep id>* **down**

Syntax Description

<name>	Specifies the MEP's maintenance domain.
<name>	Specifies the MEP's maintenance association.
<mep id>	Specifies the unique numerical ID for this MEP. Range is **1** to **8191**.
none	Optional. Specifies no domain name is used.
down	Specifies the direction of the MEP.

Default Values

By default, no MEPs exist on the interface.

Command History

Release 17.4	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

For more information about Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

For more information about specific MEP configuration commands, refer to the *Ethernet OAM CFM Command Set on page 4405*.

Usage Examples

The following example creates an MEP, with the MEP ID **100**, on the MEF Ethernet interface **0/1**. The MEP is associated with maintenance domain **Domain1** and association **association1**:

```
(config)#interface mef-ethernet 0/1
(config-mef-ethernet 0/1)#ethernet-cfm mep Domain1 association1 100 down
(config-mef-ethernet 0/1-mep)
```


ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group *<ipv4 acl name>* **in**
ip access-group *<ipv4 acl name>* **out**

Syntax Description

<ipv4 acl name>	Applies the named IPv4 ACL to the interface.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example configures the router to only allow Telnet traffic (as defined in the user-configured **TelnetOnly** ACL) into the MEF Ethernet interface:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip access-group TelnetOnly in**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii *<string>* **| hex** *<value>***] [client-id [***<interface>* **|** *<identifier>***]] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp client-id [*<interface>* **|** *<identifier>***] [hostname** *<"string">***] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp hostname *"<string>"* **[no-default-route | no-domain-name | no-nameservers] [track** *<name>***] [***<administrative distance>***]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track *<name>***] [***<administrative distance>***]**
ip address dhcp track *<name>* **[***<administrative distance>***]**

Syntax Description

<administrative distance>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii *<string>*	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex *<value>*	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<interface>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<identifier>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the *<identifier>* option.
hostname *<"string">*	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

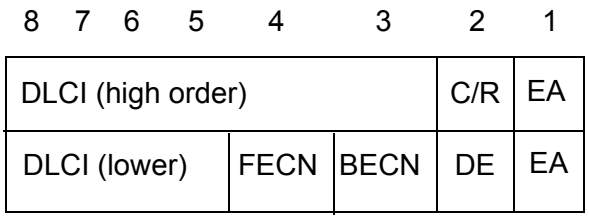
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *"<string>"* — By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip address dhcp hostname "adtran" no-default-route no-domain-name no-nameservers 5**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface (only one primary address is allowed). Use the optional **secondary** keyword to define a secondary IP address. Use the **no** form of this command to remove a configured IP address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the specified interface.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 /30**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip address 192.22.72.101 /30 secondary**

ip address range *<start ip address> <end ip address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the specified interface. Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).

Usage Examples

The following example releases the IPv4 address assigned (by DHCP) on the MEF Ethernet interface 0/1:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip dhcp release**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Optional. Specifies IP access control list (ACL) name to filter traffic.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this interface is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this interface subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this interface is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the interface **mef-ethernet 0/1**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip directed-broadcast**

ip ffe

Use the **ip ffe** command to enable the RapidRoute Engine on this interface with the default number of entries. Use the **no** form of this command to disable this feature. Variations of this command include:

ip ffe
ip ffe max-entries <*value*>

Issuing this command will cause all RapidRoute entries on this interface to be cleared.

Syntax Description

max-entries <*value*>	Optional. Specifies the maximum number of entries stored in the flow table. Valid range is from **1** to **8192**.

Default Values

By default, the RapidRoute Engine is disabled. The default number of **max-entries** is **4096**.

Command History

Release 13.1	Command was introduced.
Release 17.6	Command was expanded to include the high level data link control (HDLC) and tunnel interfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

RapidRoute can be used to help reduce routing overhead, and thus reduce overall routing times. Routing times are reduced by the creation of a flow table on the ingress interface. The maximum number of entries that can be stored in the flow table at any one time may be specified by using the **max-entries** parameters.

Usage Examples

The following example enables RapidRoute and sets the maximum number of entries in the flow table to **50**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip ffe max-entries 50**

Technology Review

The RapidRoute system goal is to increase IP packet throughput by moving as much of the packet processing into the engine as possible. Packets are classified into flows based upon the IP protocol (Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), etc.), the source and destination IP addresses, IP type of service (ToS), and the protocol-specific information, such as the source and destination port numbers. Flows are defined as the unidirectional representation of a conversation between two IP hosts. Each ingress interface keeps its own flow table, a collection of flow entries.

The first packet in a flow that is forwarded through the unit will build a flow entry. When a flow entry is looked up but no entry is found, a RapidRouteBuilder object is allocated and attached to the packet. As the packet passes through the various processing layers, each subsystem will add processing to the RapidRouteBuilder. When packet is about to be forwarded out of the egress interface, the RapidRouteBuilder will be finalized. That is, the flow entry being built will be checked for completeness and committed to the flow table on the ingress interface. Subsequent flow matches can then bypass the normal processing layers.

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on an interface. Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example enables traffic monitoring on a MEF Ethernet interface to monitor **incoming** traffic through an ACL called **myacl**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip flow ingress myacl**

ip helper-address *<ip address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

*The **ip helper-address** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets.*

Syntax Description

<ip address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (**255.255.255.255**) or a subnet broadcast (for example, **192.33.4.251** for the **192.33.4.248 /30** subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IP address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip helper-address 192.33.5.99**

ip igmp

Use the **ip igmp** command to configure multicasting related functions for the interface. Variations of this command include:

ip igmp immediate-leave
ip igmp last-member-query-interval <*milliseconds*>
ip igmp querier-timeout <*seconds*>
ip igmp query-interval <*seconds*>
ip igmp query-max-response-time <*seconds*>
ip igmp static-group <*address*>
ip igmp version [1 | 2]

Syntax Description

immediate-leave	Specifies that if only one host (or Internet Group Management Protocol (IGMP) snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured. Use the **no** form of this command to disable the **immediate-leave** feature.
last-member-query-interval <*milliseconds*>	Controls the timeout (in milliseconds) used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range is **100** to **65535** ms. Use the **no** form of this command to return to the default setting.
querier-timeout <*seconds*>	Specifies the interval (in seconds) that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range is **60** to **300** seconds. Use the **no** form of this command to return to the default setting.
query-interval <*seconds*>	Specifies the interval (in seconds) at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP time to live (TTL) of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router (DR) for the attached segment (if more than one multicast router exists). Only the DR for the segment sends queries. For IGMP V2, the DR is the router with the lowest IP address on the segment. Range is **0** to **65535** seconds. Use the **no** form of this command to return to the default setting.
query-max-response-time <*seconds*>	Specifies the maximum response time (in seconds) advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Use the **no** form of this command to return to the default setting.

Syntax Description

static-group <*address*>	Configures the router's interface to be a statically connected member of the specified group. Packets received on the correct reverse path forwarding (RPF) interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP. Use the **no** form of this command to remove a configured static group.
version [1 | 2]	Sets the interface's IGMP version. Use the **no** form of this command to return to the default setting.

Default Values

The defaults for this command are:

last-member-query-interval	**1000** milliseconds
querier-timeout	2x the **query-interval** value
query-interval	**60** seconds
query-max-response-time	**10** seconds
version	Version **1**

There are no default values for **immediate-leave** and **static-group**.

Command History

Release 7.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example sets the query message interval on the MEF Ethernet interface to **200** milliseconds:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip igmp last-member-query-interval 200**

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and Internet Group Management Protocol (IGMP) (router mode) on an interface, and to place it in multicast stub downstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router (DR) and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub upstream on page 3636* for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip mcast-stub downstream**

ip mcast-stub fixed

Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface after enabling multicast routing. Use the **no** form of this command to disable this mode.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 12.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Multicast routing must be enabled prior to setting **ip mcast-stub fixed** on the selected interface. Also, use the **ip igmp static-group** <*ip address*> command to receive multicast traffic without host-initiated Internet Group Management Protocol (IGMP) activity on the selected interface. Otherwise, all host-initiated IGMP transactions will enter multicast routes on the router's interface involved with IGMP activities.

Usage Examples

The following example enables multicast traffic forwarding and IGMP on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip mcast-stub fixed**

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 8.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address**, **ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address> on page 1418*, *ip mcast-stub downstream on page 3633*, and *ip mcast-stub upstream on page 3636* for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip mcast-stub helper-enable**

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 7.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the Internet Group Management Protocol (IGMP) host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address> on page 1418* and *ip mcast-stub downstream on page 3633* for more information.

Usage Examples

The following example enables multicast forwarding on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip mcast-stub upstream**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces	(all types)1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.

Functional Notes

Open shortest path first (OSPF) will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the MEF Ethernet interface 0/1:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip mtu 1200**

ip ospf

Use the **ip ospf** command to customize open shortest path first (OSPF) settings (if needed). Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf authentication-key <*password*>
ip ospf cost <*value*>
ip ospf dead-interval <*seconds*>
ip ospf hello-interval <*seconds*>
ip ospf message-digest-key [1 | 2] md5 <*key*>
ip ospf priority <*value*>
ip ospf retransmit-interval <*seconds*>
ip ospf transmit-delay <*seconds*>

Syntax Description

authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range is **1** to **65535**.
dead-interval <*seconds*>	Sets the maximum interval (in seconds) allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range is **0** to **32767** seconds.
hello-interval <*seconds*>	Specifies the interval (in seconds) between hello packets sent on the interface. Range is **0** to **32767** seconds.
message-digest-key [1 | 2] md5 <*key*>	Configures OSPF message digest 5 (MD5) authentication (16 byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router (DR) for this network. Range is **0** to **255**.
retransmit-interval <*seconds*>	Specifies the interval (in seconds) between link state advertisements (LSAs). Range is **0** to **32767** seconds.
transmit-delay <*seconds*>	Sets the estimated time (in seconds) required to send a link state advertisement (LSA) on the interface. Range is **0** to **32767** seconds.

Default Values

The defaults for this command are:

dead-interval <*seconds*>	40 seconds
hello-interval <*seconds*>	10 seconds: Ethernet, Frame Relay, and Point-to-Point Protocol (PPP)
priority <*value*>	1
retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example specifies an OSPF priority of **120** on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip ospf priority 120**

ip ospf authentication

Use the **ip ospf authentication** command to authenticate an interface that is performing open shortest path first (OSPF) authentication. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf authentication
ip ospf authentication message-digest
ip ospf authentication null

Syntax Description

message-digest	Optional. Selects message-digest authentication type.
null	Optional. Specifies that no authentication is used.

Default Values

By default, this is set to **null** (meaning no authentication is used).

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example specifies that no authentication will be used on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip ospf authentication null**

ip ospf network

Use the **ip ospf network** command to specify the type of network on this interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

ip ospf network broadcast
ip ospf network point-to-point

Syntax Description

broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to **broadcast**. Point-to-Point Protocol (PPP) and Frame Relay default to point-to-point.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip ospf network broadcast**

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

PIM sparse mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a rendezvous point (RP) for a multicast group or a shortest path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip pim sparse-mode**

ip pim-sparse dr-priority <*value*>

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the router's priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the priority of this interface (to be used when determining the DR). Valid range is **1** to **4294967295**.

Default Values

By default, the priority of all protocol-independent multicast (PIM) interfaces is **1**.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Interfaces advertise their configured priority values in the hello messages transmitted on the interface. Routers use the priority values to determine the appropriate DR. The router on the network segment with the highest priority is selected as the DR. If a hello message is received on the interface from a router on the network segment and it does not contain a priority, the entire network segment defaults to DR selection based on IP addresses instead of priority. In this instance, the DR is selected as the router on the network segment that has the highest IP address. AOS will always include a priority in all transmitted hello messages. If no priority is specifically designated by the user, the priority is set as the default of 1.

Usage Examples

The following example specifies a priority of **100** on the MEF Ethernet 0/1 interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip pim-sparse dr-priority 100**

ip pim-sparse hello-timer <*value*>

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the interval (in seconds) at which periodic hellos are sent out of the interface. Valid range is **10** to **3600** seconds.

Default Values

By default, the hellos are transmitted on PIM interfaces every **60** seconds.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Hello messages are used to inform neighbors of a router's presence. Hello messages normally generate a small amount of traffic on an interface. Setting the **hello-timer** to a small interval increases the number of hellos sent (thus increasing the amount of traffic). Set the **hello-timer** to a reasonable value, taking into consideration the bandwidth available on the interface.

Usage Examples

The following example specifies hellos be sent on the MEF Ethernet 0/1 interface every **3600** seconds:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip pim-sparse hello-timer 3600**

ip pim-sparse nbr-timeout <*value*>

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is **30** to **10800** seconds.

Default Values

By default, the nbr-timeout is set to **105** seconds.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example sets the neighbor timeout to **300** seconds:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip pim-sparse nbr-timeout 300**

ip pim-sparse override-interval <*value*>

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the local area network (LAN) may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the delay time in milliseconds. Valid range is **0** to **65535** milliseconds.

Default Values

By default, the override interval is set to **2500** milliseconds.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example sets the override interval to **3000** milliseconds:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip pim-sparse override-interval 3000**

ip pim-sparse propagation-delay *<value>*

Use the **ip pim-sparse propagation-delay** command to specify the expected propagation delay for join/prune messages. Set the propagation delay (in milliseconds) to estimate the amount of delay found in the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the expected propagation delay in the local link in milliseconds. Valid range is **0** to **32767** milliseconds.

Default Values

By default, the propagation delay is set to **500** milliseconds.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example sets the propagation delay to **300** milliseconds:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip pim-sparse propagation-delay 300**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example assigns the policy route map **policy1** to the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip proxy-arp**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the interface. Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only RIP version 1 packets received on the interface.
2	Accepts only RIP version 2 packets received on the interface.

Default Values

By default, all interfaces implement RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only accepts one version (either **1** or **2**) on a given interface.

Usage Examples

The following example configures the MEF Ethernet interface to accept only RIP version **2** packets:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the interface. Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only transmits one version (either **1** or **2**) on a given interface.

Usage Examples

The following example configures the MEF Ethernet interface to transmit only RIP version **2** packets:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip rip send version 2**

ip rip summary-address *<ip address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out a specified interface. Use the **no** form of this command to disable this mode.

Syntax Description

<ip address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IP address:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip route-cache**

ip urlfilter *<name>*

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the interface for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from an interface. Variations of this command include:

ip urlfilter *<name>* **in**
ip urlfilter *<name>* **out**

Syntax Description

<name>	Specifies the URL filter name to use on the interface.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any interfaces.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** *<filtername>* **http** command before applying it to the interface. Refer to *ip urlfilter allowmode on page 1493* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the MEF Ethernet interface and matches the URL filter named **MyFilter**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#ip urlfilter MyFilter in**

lldp receive

Use the **lldp receive** command to allow Link Layer Discovery Protocol (LLDP) packets to be received on this interface. Use the **no** form of this command to prevent LLDP packets from being received on the interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Command History

Release 8.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example configures the MEF Ethernet interface 0/1 to receive LLDP packets:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#lldp receive**

lldp send

Use the **lldp send** command to configure this interface to transmit Link Layer Discovery Protocol (LLDP) packets or to control the types of information contained in the LLDP packets transmitted by this interface. Use the **no** form of this command to prevent certain information from being transmitted by the interface. Variations of this command include:

lldp send 802.3-info mac-phy-config
lldp send management-address
lldp send med-info network-policy
lldp send port-description
lldp send system-capabilities
lldp send system-description
lldp send system-name
lldp send-and-receive

Syntax Description

802.3-info mac-phy-config	Enables transmission of the capability and settings of the duplex and speed on this interface.
management-address	Enables transmission of management address information on this interface.
med-info network-policy	Enables transmission of LLDP-Media Endpoint Discovery (LLDP-MED) network policy information on the interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets. This is the default setting.

Default Values

By default, all interfaces that support LLDP except routed Ethernet are configured to transmit and receive LLDP packets. LLDP is disabled by default on routed Ethernet interfaces.

The 802.3 MAC/PHY status configuration and LLDP-MED network policy time length values (TLVs) are only supported on switchport interfaces and NetVanta 1524ST Gigabit Ethernet interfaces.

Command History

Release 8.1	Command was introduced.
Release 17.2	Command was expanded to include the 802.3 and LLDP-MED information.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send-and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the MEF Ethernet interface 0/1 to transmit LLDP packets containing all enabled information types:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#lldp send**

The following example configures the MEF Ethernet interface 0/1 to transmit and receive LLDP packets containing all enabled information types:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#lldp send-and-receive**

mac-address *<mac address>*

Use the **mac-address** command to specify the medium access control (MAC) address of the unit. Only the last three values of the MAC address can be modified. The first three values contain the Adtran reserved number (00:0A:C8) by default. Use the **no** form of this command to return to the default MAC address programmed by Adtran.

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

Default Values

A unique default MAC address is programmed in each unit shipped by Adtran.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Gigabit Ethernet interfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example configures a MAC address of **00:0A:C8:5F:00:D2**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#mac-address 00:0A:C8:5F:00:D2**

max-reserved-bandwidth *<value>*

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<value>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.

Usage Examples

The following example specifies **85** percent of the bandwidth on the MEF Ethernet subinterface 0/1.1 be available for use in user-defined queues:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#max-reserved-bandwidth 85**

media-gateway ip

Use the **media-gateway ip** command to associate an Internet Protocol version 4 (IPv4) address source to use for Realtime Transport Protocol (RTP) traffic. When configuring Voice over Internet Protocol (VoIP), RTP traffic must have an IPv4 address associated with it. However, some interfaces allow dynamic configuration of IPv4 addresses, causing this value to change periodically. Use the **no** form of this command to disable this function. Variations of this command include:

media-gateway ip loopback <*interface id*>
media-gateway ip primary
media-gateway ip secondary <*ipv4 address*>

Syntax Description

loopback <*interface id*>	Specifies an IPv4 address statically defined to a loopback interface for RTP traffic. This is helpful when using a single IPv4 address across multiple wide area network (WAN) interfaces for RTP traffic. The valid range for loopback interface identifiers is **1** to **1024**. The interface ID is used to uniquely identify a loopback interface. The entered value cannot be in use by another loopback interface.
primary	Specifies using this interface's configured primary IPv4 address for RTP traffic. Applies to static, Dynamic Host Configuration Protocol (DHCP), or negotiated addresses.
secondary <*ipv4 address*>	Specifies using this interface's statically defined secondary IPv4 address for RTP traffic. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, **media-gateway ip** is disabled.

Command History

Release 10.1	Command was introduced.
Release 17.3	Command was updated with the loopback interface identification option.
Release A3.01	Command was expanded to include the Metro Ethernet forum (MEF) Ethernet interface.

Usage Examples

The following example configures the unit to use the primary IPv4 address for RTP traffic:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#media-gateway ip primary**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in *<name>*
qos-policy out *<name>*

Syntax Description

<name>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair queue to use weighted fair queuing (WFQ).
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example enables RTP quality monitoring on the MEF Ethernet 0/2 interface:

(config)**#interface mef-ethernet 0/2**
(config-mef-ethernet 0/2)**#rtp quality-monitoring**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Usage Examples

The following example enables SNMP capability on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the MEF Ethernet interface:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#no snmp trap link-status**

subtended-host mode

Use the **subtended-host mode** command to enable or disable subtended host listening on the interface. This command allows the interface to receive pre-provisioning information from another AOS unit. Variations of this command include:

subtended-host mode disabled
subtended-host mode listener

Syntax Description

disabled	Disables the interface from receiving any pre-provisioning information from another unit.
listener	Enables the interface to receive pre-provisioning information from another unit.

Default Values

By default, the first configured MEF Ethernet interface has pre-provisioning listening enabled. In addition, the Gigabit Ethernet interface **0/1** and EFM group **1/1** interfaces have pre-provisioning listening enabled by default. Any additional interfaces have pre-provisioning listening disabled.

Command History

Release A4.05	Command was introduced.
Release R11.1.0	Command was expanded to include the Gigabit Ethernet and EFM group interfaces.

Functional Notes

Only one interface at a time can have the subtended-host mode set to **listener**. If all interfaces have a subtended-host mode of **disabled**, then all pre-provisioning information is discarded.

Usage Examples

The following example enables the MEF Ethernet interface 0/1 to receive subtended-host provisioning:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)#subtended-host mode listener

traffic-shape rate <*value*>

Use the **traffic-shape rate** command to specify and enforce an output bandwidth for Ethernet and virtual local area network (VLAN) interfaces. Variations of this command include:

traffic-shape rate <*value*>
traffic-shape rate <*value*> **count-eth-overhead**
traffic-shape rate <*value*> <*burst*>
traffic-shape rate <*value*> <*burst*> **count-eth-overhead**

Syntax Description

<*value*>	Specifies the rate (in bits per second) at which the interface should be shaped.
<*burst*>	Optional. Specifies the allowed burst in bytes. By default, the burst is specified as the rate divided by 5 and represents the number of bytes that would flow within 200 ms.
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.

Default Values

By default, traffic-shaping rate is disabled.

Command History

Release 10.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.1.0	Command was expanded to include the **count-eth-overhead** parameter, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

Traffic shaping can be used to limit an Ethernet segment to a particular rate or to specify use of quality of service (QoS) on Ethernet or VLAN interfaces.

Usage Examples

The following example sets the outbound rate of the MEF Ethernet interface 0/1 to 128 kbps and applies a QoS policy that gives all Realtime Transport Protocol (RTP) traffic priority over all other traffic:

(config)**#qos map voip 1**
(config-qos-map)**#match ip rtp 10000 10500 all**
(config-qos-map)**#priority unlimited**
(config-qos-map)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#traffic-shape rate 128000**
(config-mef-ethernet 0/1)**#qos-policy out voip**

vlan-id <*vlan id*>

Use the **vlan-id** command to set a virtual local area network (VLAN) ID for the MEF Ethernet subinterface. Use the **no** form of this command to remove an entry. Variations of this command include:

vlan-id <*vlan id*>
vlan-id <*vlan id*> **native**

Syntax Description

<*vlan id*>	Specifies a valid VLAN interface ID number. Range is **1** to **4095**.
native	Optional. Specifies that data for that VLAN ID goes out untagged. If **native** is not specified, data for that VLAN ID goes out tagged.

Default Values

By default, no VLAN ID is set.

Command History

Release 6.1	Command was introduced.
Release A4.05	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.

Usage Examples

The following example configures a native VLAN of 5 for the MEF Ethernet subinterface 0/1.1:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vlan-id 5 native**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an interface to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the interface from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an interface's VRF association will clear all IP-related settings on that interface.

Syntax Description

<*name*>	Specifies the name of the VRF to which to assign the interface.

Default Values

By default, interfaces are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release 17.8	Command syntax was changed to remove the **ip** keyword for Adtran internetworking products.
Release R10.1.0	Command syntax was changed to remove the **ip** keyword for Adtran voice products.

Functional Notes

VRF instances must be created first before an interface can be assigned. An interface can only be assigned to one VRF, but multiple interfaces can be assigned to the same VRF.

An interface will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the MEF Ethernet interface 0/1 to the VRF instance named **RED**:

(config)**#interface mef-ethernet 0/1**
(config-mef-ethernet 0/1)**#vrf forwarding RED**

vrrp <*number*>

Use the **vrrp** command to configure Virtual Router Redundancy Protocol (VRRP) routers within a router group. Use the **no** form of this command to remove the VRRP router's configurations. Variations of this command include:

vrrp <*number*> **description** <*text*>
vrrp <*number*> **ip** <*address*>
vrrp <*number*> **ip** <*address*> **secondary**
vrrp <*number*> **preempt**
vrrp <*number*> **preempt delay minimum** <*time*>
vrrp <*number*> **priority** <*level*>
vrrp <*number*> **shutdown**
vrrp <*number*> **startup-delay** <*delay*>
vrrp <*number*> **timers advertise** <*interval*>
vrrp <*number*> **timers learn**
vrrp <*number*> **track** <*name*>
vrrp <*number*> **track** <*name*> **decrement** <*value*>

Syntax Description

<*number*>	Specifies the VRRP router group's virtual router ID (VRID) number. Range is **1** to **255**.
description <*text*>	Specifies the textual description of the VRRP router within the group.
ip <*address*>	Specifies the IP address to be used by the VRRP router. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
secondary	Optional. Specifies the entry of an additional VRRP router supported IP address.
preempt	Allows a VRRP router to preempt the current master router if its priority level is higher than the current master's.
delay minimum <*time*>	Optional. Specifies a delay (in seconds) before the specified router will attempt to preempt the current master router. Range is **0** to **255** seconds.
priority <*level*>	Specifies the configured priority level of the VRRP router. Level range is **1** to **254**.
shutdown	Disables the VRRP router.
startup-delay <*delay*>	Specifies a time delay (in seconds) before a VRRP router becomes active. Range is **0** to **255** seconds.
timers	Specifies the configuration of the VRRP timers.
advertise <*interval*>	Specifies the time (in seconds) between advertisements sent by the master router. Range is **1** to **255** seconds.
learn	Specifies that the backup VRRP router learns the advertisement interval of the master router.
track <*name*>	Specifies a change in priority level of the VRRP router based upon the specified track.

decrement <*value*>	Optional. Specifies the numerical amount to decrement the VRRP's priority level if the track transitions to a FAIL state. Decrement value range is **1** to **254**.

Default Values

By default, VRRP is enabled.

By default, a VRRP router will preempt with no additional delay.

The default configured priority for a VRRP router that is either a backup router or not the IP address owner is **100**. The default actual priority of a VRRP router that is the IP address owner is **255**.

By default, startup-delay is enabled with a default value of **35** seconds.

By default, the advertisement interval is **1** second.

By default, the default decrement value is **10**.

Command History

Release 16.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.

Functional Notes

A VRRP router may be part of more than one virtual router group. Although VRRP group VRIDs can be numbered between 1 and 255, only two VRRP routers per interface are supported.

It is recommended that the **timers advertise** setting is kept at the default value. If it is necessary to change this setting, ensure that all VRRP routers are configured with the new value, as all VRRP routers in the virtual group must have the same advertisement interval value. It is also recommended that if the **timers learn** function is enabled on one router in a virtual router group, then the **timers learn** function should be enabled on all routers in the group.

When the virtual router's specified IP address is independent of the IP addresses assigned to real interfaces on the VRRP routers, there is no IP address owner. This addressing method is preferred if object tracking will be used to monitor the network connection. The IP address used for the virtual router must be on the same subnet as either the primary or secondary IP addresses assigned to the VRRP router's real interface.

A track must be created before the **vrrp track** command can be issued. Refer to the *Network Monitor Track Command Set on page 4098* for more information on creating tracks. If a VRRP router owns the virtual router IP address, then the VRRP router's priority level cannot be decremented as a result of the track command. If object tracking will be used, it is important that no VRRP router own the virtual router IP address.

Usage Examples

The following example describes a VRRP router within virtual router group **1** as the **Default Master Router**:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vrrp 1 description Default Master Router**
The following example specifies an IP address of **10.0.0.1** for a VRRP router within virtual router group **1**:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vrrp 1 ip 10.0.0.1**

The following example specifies that the VRRP router within virtual router group **1** preempts the current master router after a **30** second delay:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vrrp 1 preempt delay minimum 30**

The following example specifies the configured priority for the VRRP router within virtual router group **1** is **254**:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vrrp 1 priority 254**

The following example disables the VRRP router within virtual router group **1**:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vrrp 1 shutdown**

The following example configures a VRRP router on group **1** to delay **45** seconds before becoming active:

(config)**#interface mef-ethernet 0/1.1**
(config-mef-ethernet 0/1.1)**#vrrp 1 startup-delay 45**

MEF EVC COMMAND SET

A Metro Ethernet Forum (MEF) Ethernet virtual connection (EVC) connects two endpoints (for example, the Ethernet in the first mile (EFM) group and the MEF Ethernet interface) and passes Ethernet service frames through these endpoints. The EVCs prevent data transfer between subscriber sites that are not part of the same EVC, thus providing data privacy and security similar to a Frame Relay or an asynchronous transfer mode (ATM) permanent virtual circuit (PVC). EVCs are configured to be part of a bonding group (EFM group).

Each EVC has an associated subscriber tag (s-tag). This tag is the service provider VLAN ID and the outer tag in Q-in-Q VLAN tagging, whose VLAN ID is unique among other EVCs in the Metro Ethernet network (MEN). This unique s-tag allows the EVC to be identified and separated from other EVCs within the MEN. The s-tag exists only within the MEN and is not transmitted from or received at the customer edge of the network. In addition, the customer-side VLAN ID can be preserved on EVC traffic across the MEN if necessary. The customer equipment (CE) VLAN ID is the VLAN ID of the MEF Ethernet subinterface on the AOS unit. This inner tag in Q-in-Q VLAN tagging can be preserved or stripped by the EFM module on both inbound and outbound frames.

The configurable attributes of the EVC include the EVC name, the MEN port to which the EVC is connected, whether the CE VLAN ID is preserved in the EVC traffic, and whether the EVC is enabled. Once these parameters are configured for the EVC, the EVC must be associated with a MEN port for traffic to flow.

For more information about EVCs and their function in MENs, refer to the configuration guide *Configuring EFM NIM2s and the MEF Ethernet Interface in AOS*, available online at https://supportcommunity.adtran.com.

EVCs are created and configured using the **mef evc** <*name*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#mef evc DATA
(config-evc-DATA)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

connect men-port efm-group <group id> on page 3675
preserve-ce-vlan on page 3676
s-tag <vlan id> on page 3677

connect men-port efm-group *<group id>*

Use the **connect men-port efm-group** command to associate the Ethernet virtual connection (EVC) with a specific Metro Ethernet network (MEN) port (Ethernet in the first mile (EFM) group) so that traffic can flow to the MEN. Use the **no** form of this command to remove the association between this EVC and the specified EFM group.

Syntax Description

<group id>	Specifies the EFM group to associate with the EVC. Valid range is **1** to **1024**.

Default Values

By default, no interfaces are connected to the EVC.

Command History

Release A3.01	Command was introduced.

Functional Notes

Multiple EVCs can be associated with a single EFM group. The EFM group must be created before associating the EVC and the group. For more information about configuring EFM groups, refer to *MEF EFM Group Command Set on page 3599*.

Usage Examples

The following example associates EVC **DATA** with EFM group **1**:

(config)**#mef evc DATA**
(config-evc-DATA)**#connect men-port efm-group 1**

preserve-ce-vlan

Use the **preserve-ce-vlan** command to specify whether the customer equipment (CE) virtual local area network (VLAN) ID is preserved in traffic outbound on the Ethernet virtual connection (EVC). Use the **no** form of this command to disable CE VLAN ID preservation.

Syntax Description

No subcommands.

Default Values

By default, the CE VLAN ID is preserved.

Command History

Release A3.01	Command was introduced.

Functional Notes

The CE VLAN ID is the ID of the VLAN on the Metro Ethernet Forum (MEF) Ethernet subinterface. A VLAN on the MEF Ethernet subinterface must be configured to preserve the CE VLAN ID. The preserved CE VLAN ID can be used for matching traffic in EVC maps, although for most applications you will not need to preserve the CE VLAN ID.

Usage Examples

The following example disables CE VLAN ID preservation for outbound traffic on EVC **DATA**:

(config)**#mef evc DATA**
(config-evc-DATA)**#preserve-ce-vlan**

s-tag *<vlan id>*

Use the **s-tag** command to specify the virtual local area network (VLAN) ID used by the service provider for the Ethernet virtual connection (EVC). This VLAN ID, the s-tag, is used by the carrier to mark outbound traffic from this EVC in the Metro Ethernet network (MEN). Use the **no** form of this command to return the s-tag value to the default.

Syntax Description

<vlan id>	Specifies ID of the service provider VLAN. Valid range is **1** to **4094**.

Default Values

By default, the s-tag is **0**, which indicates the traffic on the EVC is untagged.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies the s-tag for traffic outbound on EVC **DATA** is **20**:

(config)**#mef evc DATA**
(config-evc-DATA)**#s-tag 20**

MEF EVC MAP COMMAND SET

The Metro Ethernet Forum (MEF) Ethernet virtual connection (EVC) map is a traffic filter that matches traffic based on specific criteria and associates the traffic with a specific EVC. Each map is associated with a single EVC and user network interface (UNI), and it includes the customer virtual local area network (VLAN) ID and class of service (CoS) behavior of the traffic. Maps are used to classify traffic for a specific EVC for forwarding to a UNI, and for use by the MEF Policer Policy for rate limiting. For more information about EVCs, refer to the *MEF EVC Command Set on page 3674*. For more information about MEF Policer Policies, refer to the *MEF Policer Policy Command Set on page 3684*.

The configurable attributes of the EVC map include the map name, the UNI associated with the map, the EVC associated with the map, the matching criteria used to match traffic (includes the customer VLAN ID, customer priority bit, differentiated services code point (DSCP) bits, or untagged traffic), and the priority bits and egress queues the EVC uses for matched traffic. When determining traffic match criteria, keep in mind you can specify multiple criteria for a single map. Multiple match statements function as a logical AND.

Once these parameters are configured for the EVC map, the map must be associated with both an EVC and a UNI. The UNI in this case is the MEF Ethernet interface to which you want to map the traffic. Even if you are using 802.1q encapsulation, the main interface will be used as the UNI. EVC maps will always have two connection statements: one to an EVC and one to a UNI, unless the traffic matching the EVC map is to be discarded.

After configuring the EVC map and associating it with an EVC, you can also optionally specify 802.1p values for the s-tag of the traffic and the queue used when the traffic is sent to the Metro Ethernet network (MEN).

EVC maps are created and configured using the **mef evc-map** <*name*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#mef evc-map Map1
(config-evc-map-Map1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

connect on page 3679
connect discard on page 3680
match on page 3681
men-pri on page 3682
men-queue on page 3683

connect

Use the **connect** command to associate the Ethernet virtual connection (EVC) map with an EVC component. EVC maps must be associated with both an EVC and a user network interface (UNI) for the map to function properly. Use the **no** form of this command to remove the association between the EVC map and the EVC or the UNI. Variations of this command include:

connect evc <*name*>
connect uni mef-ethernet <*slot/port*>

Syntax Description

evc <*name*>	Specifies the EVC to which the matching traffic is mapped.
uni efm-group <*name*>	Specifies the Ethernet in the First Mile (EFM) group as the UNI from which traffic is evaluated.
uni gigabit-ethernet <*slot/port*>	Specifies the Gigabit Ethernet interface as the UNI from which traffic is evaluated.
uni mef-ethernet <*slot/port*>	Specifies the Metro Ethernet Forum (MEF) Ethernet interface as the UNI from which the traffic is evaluated.

Default Values

By default, no EVC components are connected to the EVC map.

Command History

Release A3.01	Command was introduced.

Functional Notes

EVC maps are associated with both an EVC and a UNI (MEF Ethernet interface) to specify where the traffic comes from as it is evaluated (UNI) and where it is mapped to if it matches the criteria outlined in the map (EVC). Both variations of this command must be entered as separate commands for the EVC map to function properly.

Usage Examples

The following example specifies that EVC map **Map1** is associated with MEF Ethernet interface **1/1** and with the EVC **DATA**:

(config)**#mef evc-map Map1**
(config-evc-map-Map1)**#connect uni mef-ethernet 1/1**
(config-evc-map-Map1)**#connect evc DATA**

connect discard

Use the **connect discard** command to specify that traffic matching the Ethernet virtual connection (EVC) map criteria is discarded. Using the **no** form of this command disables traffic discard.

Syntax Description

No subcommands.

Default Values

By default, no traffic is discarded.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that traffic matching the criteria outlined in EVC map **Map1** is discarded:

```
(config)#mef evc-map Map1
(config-evc-map-Map1)#connect discard
```

match

Use the **match** command to specify the traffic matching criteria used by the Ethernet virtual connection (EVC) map to identify which traffic to send to the associated EVC. Use the **no** form of this command to remove the matching criteria from the EVC map. Variations of this command include:

match ce-vlan-id <*vlan id*>
match ce-vlan-pri <*value*>
match dscp <*value*>
match untagged

Syntax Description

ce-vlan-id <*vlan id*>	Specifies that traffic with a customer equipment (CE) virtual local area network (VLAN) ID that matches the specified ID is mapped to the associated EVC. Valid range is **1** to **4095**.
ce-vlan-pri <*value*>	Specifies that traffic with a CE VLAN priority value that matches the specified value is mapped to the associated EVC. The priority value is also the CE VLAN 802.1p value. Valid range is **0** to **7**.
dscp <*value*>	Specifies that traffic matching the specified differentiated services code point (DSCP) value is mapped to the associated EVC. Valid range is **0** to **63**.
untagged	Specifies that untagged traffic is mapped to the associated EVC.

Default Values

By default, no matching criteria is specified.

Command History

Release A3.01	Command was introduced.

Functional Notes

Traffic is compared to the first criteria entered in the map's configuration. Subsequent criteria are then compared to the traffic in the order the criteria are entered. Multiple matches form a logical AND, meaning that if multiple criteria are entered in the map, the traffic must match all criteria to be matched to the EVC.

Usage Examples

The following example configures EVC map **Map1** to send all traffic with a CE VLAN ID of **5** and a DSCP value of **10** to the EVC associated with the map:

(config)**#mef evc-map Map1**
(config-evc-map-Map1)**#match ce-vlan-id 5**
(config-evc-map-Map1)**#match dscp 10**

men-pri

Use the **men-pri** command to specify the Metro Ethernet network (MEN) priority that the Ethernet virtual connection (EVC) will use for traffic matching the EVC map. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-pri inherit
men-pri <*value*>

Syntax Description

inherit	Specifies that the MEN priority value for the matched traffic is inherited from the 802.1p value of the customer equipment (CE) virtual local area network (VLAN).
<*value*>	Specifies a specific priority value is given to the matched traffic in the EVC. Valid range is **0** to **7**.

Default Values

By default, matched traffic has an inherited priority.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that traffic matching EVC map **Map1** is given a priority of **5** in the associated EVC:

(config)**#mef evc-map Map1**
(config-evc-map-Map1)**#men-pri 5**

men-queue

Use the **men-queue** command to specify the output queue used by the Ethernet virtual connection (EVC) for traffic that matches the EVC map. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-queue inherit
men-queue <*value*>

Syntax Description

inherit	Specifies that the queue used by the EVC for matched traffic is based on the Metro Ethernet network (MEN) priority setting (specified using the command *men-pri on page 3682*).
<*value*>	Specifies the queue to which the matched traffic is mapped by the EVC. Valid range is **1** to **8**.

Default Values

By default, matched traffic inherits the queue information.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that traffic matching EVC map **Map1** is queued in output queue **4**:

(config)**#mef evc-map Map1**
(config-evc-map-Map1)**#men-queue 4**

MEF POLICER POLICY COMMAND SET

The Metro Ethernet Forum (MEF) policer policy is a bandwidth-limiting profile that limits the amount of outbound traffic from the AOS unit to the Metro Ethernet network (MEN). The amount of traffic can be limited on Ethernet virtual connections (EVCs), user network interfaces (UNIs), or EVC maps based on traffic committed burst size (CBS), committed information rate (CIR), excess burst size (EBS), and excess information rate (EIR). The CBS and CIR thresholds specify the committed burst sizes and transmission rates of traffic. When these thresholds are exceeded, traffic may be dropped. The EBS and EIR thresholds specify the excess burst sizes or transmission rates (over and above the committed sizes or rates), specifying the maximum burst size or rate allowable before the traffic is dropped. In this way, the MEF policer policy functions similarly to Frame Relay policing. Properly configuring the MEF policer policy relies on specifying the name and the thresholds for the policy, and applying the policy to an EVC component (UNI, EVC, or EVC map).

MEF policer policies are created and configured using the **mef policer** <*name*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#mef policer Policy1
(config-policer-Policy1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

cbs <number> on page 3685
cir <number> on page 3686
ebs <number> on page 3687
eir <number> on page 3688
per on page 3689

cbs *<number>*

Use the **cbs** command to configure the committed burst size (CBS) for the Metro Ethernet Forum (MEF) policer policy. The CBS threshold specifies the maximum allowable number of bytes transmitted as a burst before the policer policy can drop the traffic. Use the **no** form of this command to return to the default setting.

Syntax Description

<number>	Specifies the CBS threshold in bytes. Valid range is **0** to **2147483647**.

Default Values

By default, the CBS is **0** bytes.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that MEF policer **Policy1** uses a CBS threshold of **6500000**:

(config)**#mef policer Policy1**
(config-policer-Policy1)**#cbs 6500000**

cir *<number>*

Use the **cir** command to configure the committed information rate (CIR) for the Metro Ethernet Forum (MEF) policer policy. The CIR threshold specifies the average maximum data transmission rate of traffic in kilobits per second (kbps) allowed before the traffic can be dropped. Use the **no** form of this command to return to the default setting.

Syntax Description

<number>	Specifies the CIR threshold in kbps. Valid range is **250** to **600000**.

Default Values

By default, the CIR is **600000** kbps.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that MEF policer **Policy1** uses a CIR threshold of **10000**:

(config)**#mef policer Policy1**
(config-policer-Policy1)**#cir 10000**

ebs *<number>*

Use the **ebs** command to configure the excess burst size (EBS) for the Metro Ethernet Forum (MEF) policer policy. The EBS threshold specifies the maximum number of bytes transmitted as a burst of data in excess of the committed burst size (CBS) threshold before the policer policy drops traffic. Set the CBS threshold using the command *cbs <number> on page 3685*. Use the **no** form of this command to return to the default setting.

Syntax Description

<number>	Specifies the EBS threshold in bytes. Valid range is **0** to **2147483647**.

Default Values

By default, the EBS is **0** bytes.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that MEF policer **Policy1** uses an EBS threshold of **60000**:

(config)**#mef policer Policy1**
(config-policer-Policy1)**#ebs 60000**

eir <*number*>

Use the **eir** command to configure the excess information rate (EIR) for the Metro Ethernet Forum (MEF) policer policy. The EIR threshold specifies the maximum rate in kilobits per second (kbps), over and above the committed information rate (CIR) threshold, before the policer policy drops traffic. The EIR value must be greater than or equal to the CIR value. Use the **no** form of this command to return to the default setting.

Syntax Description

<*number*>	Specifies the EIR threshold in kbps. Valid range is **250** to **600000**.

Default Values

By default, the EIR is **600000** kbps.

Command History

Release A3.01	Command was introduced.

Usage Examples

The following example specifies that MEF policer **Policy1** uses an EIR threshold of **1000**:

(config)**#mef policer Policy1**
(config-policer-Policy1)**#eir 1000**

per

Use the **per** command to apply the Metro Ethernet Forum (MEF) policer policy to an Ethernet virtual connection (EVC) component. Use the **no** form of this command to remove the policer policy from the EVC component. Variations of this command include:

per custom add-map <*name*>
per custom remove-map <*name*>
per evc <*name*>
per uni mef-ethernet <*slot/port*>

Syntax Description

custom add-map <*name*>	Adds the MEF policer policy to the named EVC map.
custom remove-map <*map*>	Removes the MEF policer policy from the named EVC map.
evc <*name*>	Applies the MEF policer policy to the named EVC.
uni mef-ethernet <*slot/port*>	Applies the MEF policer policy to the specified MEF Ethernet interface (the user network interface (UNI)).

Default Values

By default, no policer policies are applied to any EVC components.

Command History

Release A3.01	Command was introduced.

Functional Notes

When MEF policer policies are applied to an EVC, they are applied on egress traffic. When MEF policer policies are applied to a MEF Ethernet interface, they are applied on ingress traffic.

Usage Examples

The following example applies MEF policer **Policy1** to EVC map **Map1**:

(config)**#mef policer Policy1**
(config-policer-Policy1)**#per custom add-map Map1**

CARRIER ETHERNET SERVICES COMMAND SETS

This section includes the following command sets:

CARRIER ETHERNET EFM GROUP COMMAND SET

Ethernet in the first mile (EFM) groups are logical interfaces that represent an EFM bonding group. Interfaces are connected to the EFM group and provide physical links to carry bonded traffic. These groups are used in Layer 2/Layer 3 carrier Ethernet connections to the Metro Ethernet network (MEN). The EFM group operates as the MEN port for the AOS unit, allowing Ethernet virtual connections (EVCs) to be associated logically as a MEN port and to use the same interfaces for connection with the MEN.

EFM groups are created and configured using the **interface efm-group** <*slot/group*> or **interface efm-group** <*slot/group.subinterface id*> commands from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#interface efm-group 1/1
(config-efm-group 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bonding on page 3692
connect on page 3693
link <slot/port> on page 3694
snmp trap on page 3695
snmp trap link-status on page 3696
subtended-host mode on page 3697
thresholds xcv on page 3698
xcv-link-removal on page 3699

bonding

Use the **bonding** command to specify the bonding type to use with the specified Ethernet in the first mile (EFM) group. Use the **no** form of this command to return to the default setting.

Syntax Description

auto-detect	Specifies automatic detection of bonded or non-bonded links. The bonded mode is automatically set based upon the advertised mode received from the DSLAM during the initial handshake.
forced-on	Specifies using bonded service only.

Default Values

By default, bonding is set to **forced-on**.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

The first link within the EFM group to train sets the service type to bonded or non-bonded. If non-bonding service is detected, only the first link in the candidate list to train is used for service, ignoring the rest.

Usage Examples

The following example sets the EFM-bonding for EFM group **1/1** to **auto-detect**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#bonding auto-detect**

connect

Use the **connect** command to specify a physical interface to connect to the Ethernet in the first mile (EFM) group. Use the **no** form of this command to remove the connected interface from the group. Variations of this command include:

connect e1 <*slot/port*>
connect shdsl <*slot/port*>
connect t1 <*slot/port*>

Syntax Description

e1 <*slot/port*>	Specifies that an E1 interface is connected to the group.
shdsl <*slot/port*>	Specifies that a single-pair high-speed digital subscriber line (SHDSL) interface is connected to the group.
t1 <*slot/port*>	Specifies that a T1 interface is connected to the group.

Default Values

By default, no interfaces are connected to the EFM group.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the Layer 2/Layer 3 EFM group.

Usage Examples

The following example connects the SHDSL interface **e1 1/1** to EFM group **1/1**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#connect e1 1/1**

link <*slot/port*>

Use the **link** command to establish a link or range of links to an Ethernet in the first mile (EFM) group. Use the **no** form of this command to remove the link. Variations of this command include:

link <*slot/port*>
link <*slot/port-to-port*>

Syntax Description

<*slot/port*>	Specifies the slot and port to link to the EFM group.
<*slot/port-to-port*>	Specifies a range of ports to link to the EFM group.

Default Values

By default, no links are configured for EFM groups.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example links the EFM group to slot and port **1/1**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#link 1/1**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Us the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Usage Examples

The following example enables SNMP capability on the EFM group 1/1:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the EFM group 1/1:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#no snmp trap link-status**

subtended-host mode

Use the **subtended-host mode** command to enable or disable subtended host listening on the interface. This command allows the interface to receive pre-provisioning information from another AOS unit. Variations of this command include:

subtended-host mode listener
subtended-host mode disabled

Syntax Description

listener	Enables the interface to receive pre-provisioning information from another unit.
disabled	Disables the interface from receiving any pre-provisioning information from another unit.

Default Values

By default, the first configured MEF Ethernet interface has pre-provisioning listening enabled. In addition, the Gigabit Ethernet interface **0/1** and EFM group **1/1** interfaces have pre-provisioning listening enabled by default. Any additional interfaces have pre-provisioning listening disabled.

Command History

Release A4.05	Command was introduced.
Release R11.1.0	Command was expanded to include the Gigabit Ethernet and EFM group interfaces.

Functional Notes

Only one interface at a time can have the subtended-host mode set to **listener**. If all interfaces have a subtended-host mode of **disabled**, then all pre-provisioning information is discarded.

Usage Examples

The following example enables the MEF Ethernet interface 0/1 to receive subtended-host provisioning:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#subtended-host mode listener**

thresholds xcv

Use the **thresholds xcv** command to configure the excessive code violation threshold for the interface's link in the Ethernet in the first mile (EFM) group. When this threshold is crossed, the link is removed from the group. Use the **no** form of this command to return the threshold to the default value. Variations of this command include:

thresholds xcv 1e-5
thresholds xcv 1e-6
thresholds xcv 1e-7

Syntax Description

1e-5	Specifies that the threshold is set at a 1e-5 bit error rate.
1e-6	Specifies that the threshold is set at a 1e-6 bit error rate.
1e-7	Specifies that the threshold is set at a 1e-7 bit error rate.

Default Values

By default, thresholds are set to **1e-7**.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the Layer 2/Layer 3 EFM group.

Functional Notes

Once the threshold is set, the command *xcv-link-removal on page 3699* must be entered in the group's configuration so that the interface's link is removed when the threshold is crossed.

Usage Examples

The following example specifies that the excessive code violation threshold for interfaces connected to EFM group **1/1** is **1e-6**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#thresholds xcv 1e-6**

xcv-link-removal

Use the **xcv-link-removal** command to remove an interface's link from the Ethernet in the first mile (EFM) group if the excessive code violation threshold is exceeded. This threshold is set using the command *thresholds xcv on page 3698*. Using the **no** form of this command disables the link removal.

Syntax Description

No subcommands.

Default Values

By default, link removal is enabled for the EFM group.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the Layer 2/Layer 3 EFM group.

Usage Examples

The following example specifies that an interface whose excessive code violations exceed the threshold is no longer linked to EFM group **1/1**:

(config)**#interface efm-group 1/1**
(config-efm-group 1/1)**#xcv-link-removal**

CARRIER ETHERNET EVC COMMAND SET

A carrier Ethernet Ethernet virtual connection (EVC) connects two endpoints (for example, the Metro Ethernet network (MEN) port and the User Network Interface (UNI)) and passes both Layer 2 and Layer 3 Ethernet service frames through these endpoints for carrier Ethernet services. The EVCs prevent data transfer between subscriber sites that are not part of the same EVC, thus providing data privacy and security similar to a Frame Relay or an asynchronous transfer mode (ATM) permanent virtual circuit (PVC).

Each EVC has an associated subscriber tag (s-tag). This tag is the service provider VLAN ID and the outer tag in Q-in-Q VLAN tagging, whose VLAN ID is unique among other EVCs in the Metro Ethernet network (MEN). This unique s-tag allows the EVC to be identified and separated from other EVCs within the MEN. The s-tag exists only within the MEN and is not transmitted from or received at the customer edge of the network. In addition, the customer-side VLAN ID can be preserved on EVC traffic across the MEN if necessary. The customer equipment (CE) VLAN ID is the VLAN ID of the MEF Ethernet subinterface on the AOS unit. This inner tag in Q-in-Q VLAN tagging can either be preserved or stripped by the EFM module on both inbound and outbound frames.

The configurable attributes of the EVC include the EVC name, the MEN port to which the EVC is connected, whether the CE VLAN ID is preserved in the EVC traffic, and whether the EVC is enabled. Once these parameters are configured for the EVC, the EVC must be associated with a MEN port for traffic to flow.

EVCs are created and configured using the **evc** <*name*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#evc DATA
(config-evc DATA)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

connect men-port on page 3701
performance-statistics on page 3702
preserve-ce-vlan on page 3703
s-tag <vlan id> on page 3704

connect men-port

Use the **connect men-port** command to associate the Layer 2/Layer 3 Ethernet virtual connection (EVC) with a specific Metro Ethernet network (MEN) port so that traffic can flow to the MEN. Use the **no** form of this command to remove the association between this EVC and the port. Variations of this command include:

connect men-port efm-group <*slot/group*>
connect men-port gigabit-ethernet <*slot/port*>

Syntax Description

efm-group <*slot/group*>	Specifies the Ethernet in the first mile (EFM) group to associate with the EVC using the group's slot number and group ID.
gigabit-ethernet <*slot/port*>	Specifies a Gigabit Ethernet interface to associate with the EVC.

Default Values

By default, no interfaces are connected to the EVC.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the Layer 2/Layer 3 EVC and the EFM group and Gigabit Ethernet interfaces.

Functional Notes

Multiple EVCs can be associated with a single EFM group. The EFM group must be created before associating the EVC and the group. For more information about configuring EFM groups, refer to *Carrier Ethernet EFM Group Command Set on page 3691*.

Usage Examples

The following example associates EVC **DATA** with EFM group **1/1**:

(config)**#evc DATA**
(config-evc DATA)**#connect men-port efm-group 1/1**

performance-statistics

Use the **performance-statistics** command to enable gathering performance monitoring statistics on the EVC. Use the **no** form of this command to disable the performance monitoring feature.

Syntax Description

No subcommands.

Default Values

By default, performance monitoring is enabled.

Command History

Release R10.10.0	Command was introduced.
Release R11.5.0	Command expanded to include the Carrier Ethernet EVC.

Usage Examples

The following example enables performance monitoring on the EVC **DATA**:

(config)**#interface evc DATA**
(config-evc DATA)**#performance-statistics**

preserve-ce-vlan

Use the **preserve-ce-vlan** command to specify whether the customer equipment (CE) virtual local area network (VLAN) ID is preserved in traffic outbound on the Ethernet virtual connection (EVC). Use the **no** form of this command to disable CE VLAN ID preservation.

Syntax Description

No subcommands.

Default Values

By default, the CE VLAN ID is preserved.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the Layer 2/Layer 3 EVC.

Usage Examples

The following example disables CE VLAN ID preservation for outbound traffic on EVC **DATA**:

(config)**#evc DATA**
(config-evc DATA)**#no preserve-ce-vlan**

s-tag *<vlan id>*

Use the **s-tag** command to specify the virtual local area network (VLAN) ID used by the service provider for the Layer 2/Layer 3 Ethernet virtual connection (EVC). This VLAN ID, the s-tag, is used by the carrier to mark outbound traffic from this EVC in the Metro Ethernet network (MEN). Use the **no** form of this command to return the s-tag value to the default.

Syntax Description

<vlan id>	Specifies ID of the service provider VLAN. Valid range is **2** to **4094**.

Default Values

By default, the s-tag is not specified, which prevents the EVC from becoming active.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the Layer 2/Layer 3 EVC.

Usage Examples

The following example specifies the s-tag for traffic outbound on EVC **DATA** is **20**:

(config)**#evc DATA**
(config-evc DATA)**#s-tag 20**

CARRIER ETHERNET EVC MAP COMMAND SET

The carrier Ethernet Ethernet virtual connection (EVC) map is a traffic filter that matches Layer 2 traffic based on specific criteria and associates the traffic with a specific EVC for Layer 2 carrier Ethernet services. Each map is associated with a single EVC and user network interface (UNI), and it includes the customer virtual local area network (VLAN) ID and class of service (CoS) behavior of the traffic. Maps are used to classify traffic for a specific EVC for forwarding to a UNI, and for use by the EVC Policer Policy for rate limiting. For more information about EVCs, refer to the *Carrier Ethernet EVC Command Set on page 3700*. For more information about EVC Policer Policies, refer to the *Carrier Ethernet Policer Command Set on page 3719*.

The configurable attributes of the EVC map include the map name, the UNI associated with the map, the EVC associated with the map, the matching criteria used to match traffic (includes the customer VLAN ID, customer priority bit, differentiated services code point (DSCP) bits, or untagged traffic), and the priority bits and egress queues the EVC uses for matched traffic. Multiple traffic match criteria can be specified for a single map. Multiple match statements function as a logical AND.

Once these parameters are configured for the EVC map, the map must be associated with both an EVC and a UNI. The UNI in this case is the Ethernet in the first mile (EFM) group or Gigabit Ethernet interface to which you want to map the traffic. Even if you are using 802.1q encapsulation, the main interface will be used as the UNI. EVC maps will always have two connection statements: one to an EVC and one to a UNI, unless the traffic matching the EVC map is to be discarded.

After configuring the EVC map and associating it with an EVC, you can also optionally specify 802.1p values for the s-tag of the traffic and the queue used when the traffic is sent to the Metro Ethernet network (MEN).

EVC maps are created and configured using the **evc-map** <*name*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#evc-map Map1
(config-evc-map Map1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

block uni ingress-only on page 3707
ce-vlan-tpid on page 3708
connect on page 3709
connect discard on page 3710

block uni ingress-only

Use the **block uni ingress-only** command to enable ETREE traffic separation on the Ethernet virtual connection (EVC) map. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example enables ETREE traffic separation on the EVC map:

```
(config)# evc-map Map1
(config-evc-map Map1)#block uni ingress-only
```

ce-vlan-tpid

Use the **ce-vlan-tpid** command to specify that an Ethernet virtual connection (EVC) map uses the globally set customer-edge (CE) virtual local area network (VLAN) tag protocol identifier (TPID) value. Use the **no** form of this command to use the default value of 0x8100 instead of the global setting.

Syntax Description

No subcommands.

Default Values

By default, an EVC map uses the global setting.

Command History

Release R11.6.0	Command was introduced.

Functional Note

All EVC maps default to the globally-specified EtherType for CE VLAN ID matching. In addition, all EVC maps default to using the specified EtherType for adding CE VLAN IDs to traffic flowing in the Metro Ethernet Network (MEN) to UNI direction when the CE VLAN ID is not preserved as well as using the specified EtherType for adding c-tags to traffic flowing in the UNI to MEN direction. For more information, refer to the *Carrier Ethernet Services in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the EVC map uses the default setting instead of the global setting:

```
(config)# evc-map Map1
(config-evc-map Map1)#no ce-vlan-tpid
```

connect

Use the **connect** command to associate the Ethernet virtual connection (EVC) map with an EVC component. EVC maps must be associated with both an EVC and a user network interface (UNI) for the map to function properly. Use the **no** form of this command to remove the association between the EVC map and the EVC or the UNI. Variations of this command include:

connect evc <*name*>
connect uni efm-group <*slot/group*>
connect uni gigabit-ethernet <*slot/port*>

Syntax Description

evc <*name*>	Specifies the EVC to which the matching traffic is mapped.
uni efm-group <*slot/group*>	Specifies the Ethernet in the First Mile (EFM) group as the UNI from which traffic is evaluated.
uni gigabit-ethernet <*slot/port*>	Specifies the Gigabit Ethernet interface as the UNI from which traffic is evaluated.

Default Values

By default, no EVC components are connected to the EVC map.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet EVC Map and the **uni efm-group** and **uni gigabit-ethernet** parameters.

Functional Notes

EVC maps are associated with both an EVC and a UNI (Gigabit Ethernet interface) to specify where the traffic comes from as it is evaluated (UNI) and where it is mapped to if it matches the criteria outlined in the map (EVC). Both variations of this command must be entered as separate commands for the EVC map to function properly.

Usage Examples

The following example specifies that EVC map **Map1** is associated with Gigabit Ethernet interface **1/1** and with the EVC **DATA**:

(config)**# evc-map Map1**
(config-evc-map Map1)**#connect uni gigabit-ethernet 1/1**
(config-evc-map Map1)**#connect evc DATA**

connect discard

Use the **connect discard** command to specify that traffic matching the Ethernet virtual connection (EVC) map criteria is discarded. Using the **no** form of this command disables traffic discard.

Syntax Description

No subcommands.

Default Values

By default, no traffic is discarded.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet EVC map.

Usage Examples

The following example specifies that traffic matching the criteria outlined in EVC map **Map1** is discarded:

(config)**#mef evc-map Map1**
(config-evc-map Map1)**#connect discard**

match

Use the **match** command to specify the traffic matching criteria used by the Ethernet virtual connection (EVC) map to identify which traffic to send to the associated EVC. Use the **no** form of this command to remove the matching criteria from the EVC map. Variations of this command include:

match broadcast
match ce-vlan-id <*vlan id*>
match ce-vlan-pri <*value*>
match dscp <*value*>
match l2cp
match multicast
match unicast
match untagged

Syntax Description

broadcast	Specifies that broadcast traffic is mapped to the associated EVC.
ce-vlan-id <*vlan id*>	Specifies that traffic with a customer equipment (CE) virtual local area network (VLAN) ID that matches the specified ID is mapped to the associated EVC. VLAN IDs can be a single ID, multiple IDs, or a range of IDs. Multiple VLAN IDs should be separated with a comma (**600,200,800**). A range can be specified with a hyphen (**400-500**).Valid range is **1** to **4094**.
ce-vlan-pri <*value*>	Specifies that traffic with a CE VLAN priority value that matches the specified value is mapped to the associated EVC. The priority value is also the CE VLAN 802.1p value. Valid range is **0** to **7**.
dscp <*value*>	Specifies that IPv4 and IPv6 traffic matching the specified differentiated services code point (DSCP) value is mapped to the associated EVC. Valid range is **0** to **63**.
l2cp	Specifies that L2CP traffic is mapped to the associated EVC.
multicast	Specifies that multicast traffic is mapped to the associated EVC.
unicast	Specifies that unicast traffic is mapped to the associated EVC.
untagged	Specifies that untagged traffic is mapped to the associated EVC.

Default Values

By default, all traffic on the connected user network interface (UNI) port is matched.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the EVC map and the **broadcast**, **12cp**, **multicast**, and **unicast** parameters.
Release R11.6.0	Command was expanded to include support for matching on multiple CE VLAN IDs.

Functional Notes

Traffic is compared to the first criteria entered in the map's configuration. Subsequent criteria are then compared to the traffic in the order the criteria are entered. Multiple matches form a logical AND, meaning that if multiple criteria are entered in the map, the traffic must match all criteria to be matched to the EVC.

In AOS firmware release R11.6.0, support for matching multiple VLANs to a single EVC map was added. This feature is available on Gigabit Ethernet ports configured as UNIs on Carrier Ethernet products. Identical VLAN bundles (a set of multiple VLAN IDs) can exist on two or more different EVC maps, provided there is at least one additional match criteria that allows the EVC maps to become active. Different VLAN bundles that overlap on two EVC maps on the same UNI are not allowed and will prevent both EVC maps from becoming active. For example, one EVC map with VLAN IDs 201-400 conflicts with another EVC map with VLAN IDs 301-500 if they are on the same UNI since VLAN IDs 301-400 are overlapping in both VLAN bundles.

Usage Examples

The following example configures EVC map **Map1** to send all traffic with a CE VLAN ID of **5** and a DSCP value of **10** to the EVC associated with the map:

(config)**#evc-map Map1**
(config-evc-map Map1)**#match ce-vlan-id 5**
(config-evc-map Map1)**#match dscp 10**

match destination mac address <*mac address*>

Use the **match destination mac address** command to specify a media access control (MAC) address to use as matching criteria in the Ethernet virtual connection (EVC) map. Use the **no** form of this command to remove this criteria from the map.

Syntax Description

<*mac address*>	Specifies the MAC address to use for matching. MAC addresses are specified in the format **HH:HH:HH:HH:HH:HH**.

Default Values

By default, no MAC addresses are associated with the EVC map.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example specifies the EVC map matches destination MAC address **00:A0:C8:00:00:01**:

(config)**# evc-map Map1**
(config-evc-map Map1)**#match destination mac address 00:A0:C8:00:00:01**

match ethertype *<value>*

Use the **match ethertype** command to specify an EtherType filter to use as matching criteria on the Ethernet virtual connection (EVC) map. EtherType filters allow you to specify a certain EtherType (such as Address Resolution Protocol (ARP) or Internet Protocol version 6 (IPv6)) as EVC map matching criteria for allowed traffic into the UNI interface. This feature can also be configured to drop certain EtherTypes by associating an EVC map with a discard type, rather than a valid EVC. Use the **no** form of this command to remove the matching criteria from the EVC map.

Syntax Description

<value>	Specifies an EtherType, in hexadecimal format, to use as matching criteria in the EVC map.

Default Values

By default, no EtherType matching is configured.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example specifies that ARP is used as a matching criteria in the EVC map:

(config)**# evc-map Map1**
(config-evc-map Map1)**#match ethertype 0x0806**

men-c-tag <*value*>

Use the **men-c-tag** command to specify that the C-tag is inserted on the matching packets as they leave the Metro Ethernet network (MEN) and is used to further identify traffic on the Ethernet virtual connection (EVC). Use the **no** form of this command to remove the C-tag value.

Syntax Description

<*value*>	Specifies the value for the C-tag. Valid range is **2** to **4094**.

Default Values

By default, the C-tag is not specified.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies a C-tag value of **100** for the traffic associated with the EVC map **Map1**:

(config)**#evc-map Map1**
(config-evc-map Map1)**#men-c-tag 100**

men-c-tag-pri

Use the **men-c-tag-pri** command to specify the 802.1p value of the C-tag. The C-tag is used to identify traffic within an Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default value. Variations of this command include:

men-c-tag-pri inherit
men-c-tag-pri <*value*>

Syntax Description

inherit	Specifies that the C-tag 802.1p value for the matched traffic is inherited from the 802.1p value of the customer edge (CE) virtual local area network (VLAN).
<*value*>	Specifies the C-tag priority. Valid range is **0** to **7**.

Default Values

By default, the C-tag priority is set to **inherit**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies the C-tag priority as **6** on EVC map **Map1**:

(config)**#evc-map Map1**
(config-evc-map Map1)**#men-c-tag-pri 6**

men-pri

Use the **men-pri** command to specify the 802.1p value to the service virtual local area network (VLAN) tag (S-tag) that the Ethernet virtual connection (EVC) will use for traffic matching the EVC map. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-pri inherit
men-pri <*value*>

Syntax Description

inherit	Specifies that the S-tag priority value for the matched traffic is inherited from the 802.1p value of the customer edge (CE) VLAN.
<*value*>	Specifies a specific priority value is given to the matched traffic in the EVC. Valid range is **0** to **7**.

Default Values

By default, matched traffic has an inherited priority.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet EVC map.

Usage Examples

The following example specifies that traffic matching EVC map **Map1** is given a priority of **5** in the associated EVC:

(config)**#evc-map Map1**
(config-evc-map Map1)**#men-pri 5**

men-queue

Use the **men-queue** command to specify the output queue used by the Ethernet virtual connection (EVC) for traffic that matches the EVC map. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-queue inherit
men-queue <*value*>

Syntax Description

inherit	Specifies that the queue used by the EVC for matched traffic is based on the Metro Ethernet network (MEN) priority-to-queue mapping.
<*value*>	Specifies the queue to which the matched traffic is mapped by the EVC. Valid range is **0** to **7**.

Default Values

By default, matched traffic inherits the queue information.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet EVC map.

Usage Examples

The following example specifies that traffic matching EVC map **Map1** is queued in output queue **4**:

(config)**#evc-map Map1**
(config-evc-map Map1)**#men-queue 4**

CARRIER ETHERNET POLICER COMMAND SET

The policer is a bandwidth limiting profile that limits the amount of outbound traffic from the AOS unit to the Metro Ethernet network (MEN). The amount of traffic can be limited on Ethernet virtual connections (EVCs), user network interfaces (UNIs), or EVC maps based on traffic committed burst size (CBS), committed information rate (CIR), excess burst size (EBS), and excess information rate (EIR). The CBS and CIR thresholds specify the committed burst sizes and transmission rates of traffic. When these thresholds are exceeded, traffic can be dropped. The EBS and EIR thresholds specify the excess burst sizes or transmission rates (over and above the committed sizes or rates), specifying the maximum burst size or rate allowable before the traffic is dropped. In this way, the EVC policer functions similarly to Frame Relay policing. Traffic can also go through a second tier of policing in order to limit the overall rate or burst size in addition to the first tier policing of individual services. Properly configuring the policer relies on specifying the name and the thresholds for the policy, and applying the policy to a component (UNI, EVC, or EVC map) or a first tier policer.

Policers are created and configured using the **policer** <*name*> **[**<*slot*>**]** command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#policer Policer1
(config-policer Policer1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

cbs <number> on page 3720
cir <number> on page 3721
color-aware on page 3722
coupling on page 3723
ebs <number> on page 3724
eir <number> on page 3725
per on page 3726

cbs *<number>*

Use the **cbs** command to configure the committed burst size (CBS) for the policer. The CBS threshold specifies the maximum allowable number of bytes transmitted as a burst before the policer drops the traffic. Use the **no** form of this command to return to the default setting.

Syntax Description

<number>	Specifies the CBS threshold in bytes. Valid range is **0** to **999999**.

Default Values

By default, the CBS is **3125** bytes.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet policer.

Usage Examples

The following example specifies that EVC policer **Policer1** uses a CBS threshold of **6500**:

(config)**#policer Policer1**
(config-policer Policer1)**#cbs 6500**

cir *<number>*

Use the **cir** command to configure the committed information rate (CIR) for the policer. The CIR threshold specifies the average maximum data transmission rate of traffic in kilobits per second (kbps) allowed before the traffic is dropped. Use the **no** form of this command to return to the default setting.

Syntax Description

<number>	Specifies the CIR threshold in kbps. Valid range is **250** to **100000**.

Default Values

By default, the CIR is **0** kbps.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet policer.

Usage Examples

The following example specifies that policer **Policer1** uses a CIR threshold of **10000**:

```
(config)#policer Policer1
(config-policer Policer1)#cir 10000
```

color-aware

Use the **color-aware** command to enable the policer to consider color marking when examining incoming packets. When enabled, the policer takes the color marking of a packet into consideration when determining the new color marking. Incoming green packets can be declared green, yellow, or red (dropped) by a color-aware policer. Incoming yellow packets can only be declared yellow or red. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the policer pays no attention to color marking.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example specifies that policer **Policer1** examines color markings:

(config)**#policer Policer1**
(config-policer Policer1)**#color-aware**

coupling

Use the **coupling** command to couple internal operation for token refills from the committed information rate (CIR) to excess information rate (EIR) buckets for the policer. Tokens that cannot fill the green bucket when it is full (i.e., when no green traffic is currently running) will overflow into the yellow bucket so that yellow traffic is processed at a rate of CIR + EIR. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, coupling is disabled.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Coupling should be used with a policer that is color aware. Coupling will have little effect on a policer that has **color-aware** disabled.

Usage Examples

The following example enables coupling for the policer **Policer1**:

```
(config)#policer Policer1
(config-policer Policer1)#coupling
```

ebs *<number>*

Use the **ebs** command to configure the excess burst size (EBS) for the policer. The EBS threshold specifies the maximum number of bytes transmitted as a burst of data in excess of the committed burst size (CBS) threshold before the policer policy drops traffic. Set the CBS threshold using the command *cbs <number> on page 3720*. Use the **no** form of this command to return to the default setting.

Syntax Description

<number>	Specifies the EBS threshold in bytes. Valid range is **0** to **999999**.

Default Values

By default, the EBS is **12500** bytes.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet policer.

Usage Examples

The following example specifies that policer **Policer1** uses an EBS threshold of **60000**:

(config)**#policer Policer1**
(config-policer Policer1)**#ebs 60000**

eir *<number>*

Use the **eir** command to configure the excess information rate (EIR) for the policer. The EIR threshold specifies the maximum rate in kilobits per second (kbps), over and above the committed information rate (CIR) threshold, before the policer policy drops traffic. The EIR value must be greater than or equal to the CIR value. Use the **no** form of this command to return to the default setting.

Syntax Description

<number>	Specifies the EIR threshold in kbps. Valid range is **250** to **600000**.

Default Values

By default, the EIR is **100000** kbps.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the carrier Ethernet policer.

Usage Examples

The following example specifies that policer **Policer1** uses an EIR threshold of **10000**:

(config)**#policer Policer1**
(config-policer Policer1)**#eir 1000**

per

Use the **per** command to apply the policer to an EVC component. Use the **no** form of this command to remove the policer from the component. Variations of this command include:

per custom evc-map <*name*>
per custom interface efm-group <*slot/group.subinterface*>
per custom interface gigabit-ethernet <*slot/port.subinterface*>
per custom evc <*name*>
per policer <*name*>
per uni efm-group <*slot/group*>
per uni gigabit-ethernet <*slot/port*>

Syntax Description

custom	
evc-map <*name*>	Adds the policer to the named EVC map.
interface efm-group <*slot/group.subinterface*>	Applies the policer to all ingress traffic on the Ethernet in the first mile (EFM) group subinterface.
interface gigabit-ethernet <*slot/port.subinterface*>	Applies the policer to all ingress traffic on the Gigabit Ethernet subinterface.
evc <*name*>	Applies the policer to all EVC maps associated with the named EVC.
policer <*name*>	Specifies the policer is in **per policer** mode. The **per policer** mode identifies this policer as the second tier policer and specifies the name of the first tier policer with the parameter <*name*>. If the policer named in <*name*> doesn't exist when the command is issued, it will be created.
uni efm-group <*slot/group*>	Applies the policer to all EVC maps associated with the specified EFM group (the user network interface (UNI)).
uni gigabit-ethernet <*slot/port*>	Applies the policer to all EVC maps associated with the specified Gigabit Ethernet interface.

Default Values

By default, no policer are applied to any EVC components.

Command History

Release R10.10.0	Command was introduced.
Release R11.5.0	Command was expanded to include **per policer** <*name*> parameter.

Functional Notes

A policer can be configured to police multiple first tier policers by specifying multiple **per policer** <*name*> commands. Each new command will be added to any existing **per policer** commands in the configuration. If the policer is already configured for a different policer mode (**per uni**, **per evc**, or **per custom**), the policer mode will be changed to **per policer** and any existing **per uni**, **per evc**, or **per custom** configuration will be automatically removed.

Usage Examples

The following example applies policer **Policer1** to EVC map **Map1**:

(config)**#policer Policer1**
(config-policer Policer1)**#per custom evc-map Map1**

CARRIER ETHERNET QUEUE COMMAND SET

The carrier Ethernet Ethernet virtual connection (EVC) queue provices eight hardware queues per Metro Ethernet network (MEN) port, whether an Ethernet in the first mile (EFM) group or Gigabit Ethernet interface, allowing for traffic management and congestion avoidance. These queues absorb packets when the ingress rate of traffic exceeds the egress rate, allowing bursts of packets to be transmitted through the system without incurring loss.

Carrier ethernet EVC queues must be managed to prevent packet loss and delay along the network. From the EVC Queue Configuration mode you can specify the algorithms, class of service (CoS) settings, drop probabilities, queue depth, thresholds, and weights of traffic traversing the MEN port interface.

The EVC Queue Configuration mode is accessed using the **queue interface** command from the Global Configuration mode as follows:

```
(config)#queue interface efm-group 1/1 3
(config-queue 3)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

algorithm wred on page 3729
cos group lower-adjacent on page 3730
cos <value> on page 3731
drop-probability on page 3732
max-depth <number> on page 3733
thresholds wred on page 3734
weight on page 3735

algorithm wred

Use the **algorithm wred** command to enable weighted random early detection (WRED) in the Ethernet virtual connection (EVC) queue. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, WRED is disabled.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

WRED is an active queue congestion management discipline that adds packet color to the thresholds of the drop probability slopes for queued traffic. Different slopes can be configured to treat conforming (green colored) and nonconforming (yellow colored) packets differently. As the average queue depth increases, the AOS unit begins to randomly discard yellow packets before randomly discarding green packets. Once the maximum threshold of the average queue depth is reached, all packets are discarded. Packet color and average queue depth are used to determine drop probability.

When using WRED, make sure to configure the yellow maximum threshold to be less than or equal to the green minimum threshold (using the command *thresholds wred on page 3734*) to avoid dropping green packets before all yellow packets are dropped.

Usage Examples

The following example enables WRED in the EVC queue:

(config)**#queue interface efm-group 1/1 3**
(config-queue 3)**#algorithm wred**

cos group lower-adjacent

Use the **cos group lower-adjacent** command to lower the adjacency of the Ethernet virtual connection (EVC) queue class of service (CoS). Use the **no** form of this command to disable queue CoS adjacency.

Syntax Description

No subcommands.

Default Values

CoS adjacency is disabled by default.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example lowers the adjacency of the EVC queue CoS:

(config)**#queue interface efm-group 1/1 3**
(config-queue 3)**#cos group lower-adjacent**

cos *<value>*

Use the **cos** command to set the class of service (CoS) value for a particular Ethernet virtual connection (EVC) queue. Queues with the same CoS value enable the scheduling of packets between the same CoS queues using the deficit weighted round robin (DWRR) algorithm. Use the **no** form of this command to disable CoS for the queue.

Syntax Description

<value>	Specifies the CoS value for the queue. Valid range is **0** to **7**.

Default Values

By default, queues do not have a CoS value.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies a CoS value of **2** for the EVC queue:

(config)**#queue interface efm-group 1/1 3**
(config-queue 3)**#cos 2**

drop-probability

Use the **drop-probability** command to set the drop probability of traffic entering the Ethernet virtual connection (EVC) queue. Use the **no** form of this command to return to the default value. Variations of this command include:

drop-probability green <*value*>
drop-probability yellow <*value*>

Syntax Description

green <*value*>	Specifies the weighted random early detection (WRED) drop probability for green-colored traffic. Valid range is **0** to **100**.
yellow <*value*>	Specifies the WRED drop probability for yellow-colored traffic. Valid range is **0** to **100**.

Default Values

By default, the drop probability is set to **0**.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

When using WRED, make sure to configure the yellow maximum threshold to be less than or equal to the green minimum threshold (using the command *thresholds wred on page 3734*) to avoid dropping green packets before all yellow packets are dropped.

Usage Examples

The following example specifies the EVC queue has a drop probability of **3** for green traffic:

(config)**#queue interface efm-group 1/1 3**
(config-queue 3)**#drop-probability green 3**

max-depth *<number>*

Use the **max-depth** command to specify the maximum number of packets that can be held by the Ethernet virtual connection (EVC) queue. Use the **no** form of this command to return to the default value.

Syntax Description

<number>	Specifies the maximum number of packets that can be held by the queue. Valid range is **1** to **16383**.

Default Values

By default, the queue holds **255** packets.

Command History

Release R10.10.0	Command was introduced.
Release R11.10.2	Maximum queue depth was increased to **16383** packets.

Usage Examples

The following example specifies the EVC queue can hold a maximum of **100** packets:

(config)**#queue interface efm-group 1/1 3**
(config-queue 3)**#max-depth 100**

thresholds wred

Use the **thresholds wred** command to specify the congestion management thresholds for dropping weighted random early detection (WRED) traffic from the Ethernet virtual connection (EVC) queue. Use the **no** form of this command to return to the default setting. Variations of this command include:

thresholds wred green maximum <*value*>
thresholds wred green minimum <*value*>
thresholds wred yellow maximum <*value*>
thresholds wred yellow minimum <*value*>

Syntax Description

green	Configures the threshold for WRED conforming (green) traffic.
yellow	Configures the threshold for WRED nonconforming (yellow) traffic.
maximum <*value*>	Specifies the maximum threshold for dropping traffic. Valid range is **1** to **255**.
minimum <*value*>	Specifies the minimum threshold for dropping traffic. Valid range is **1** to **255**.

Default Values

By default, the threshold is set to **1**.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

When using WRED, make sure to configure the yellow maximum threshold to be less than or equal to the green minimum threshold to avoid dropping green packets before all yellow packets are dropped.

Usage Examples

The following example sets the maximum threshold for green traffic to **255**:

(config)**#queue interface efm-group 1/1 3**
(config-queue 3)**#thresholds wred green maximum 255**

weight

Use the **weight** command to specify the weight given to traffic for a specific Ethernet virtual connection (EVC) queue when using weighted fair queueing (WFQ). Use the **no** form of this command to return to the default setting. Variations of this command include:

weight dynamic
weight <*number*>

Syntax Description

dynamic	Specifies that traffic is weighted dynamically.
<*number*>	Assigns a percentage weight to the traffic. Valid range is **1** to **100** percent.

Default Values

By default, traffic is weighted dynamically.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that traffic for the EVC queue is weighed by **25** percent:

(config)**#queue interface efm-group 1/1 3**
(config-queue 3)**#weight 25**

CARRIER ETHERNET SHAPER COMMAND SET

The carrier Ethernet Ethernet virtual connection (EVC) traffic shaper is used to smooth bursts of traffic traveling between the AOS unit and the Metro Ethernet network (MEN). When a packet arrives at the shaper, if there are sufficient tokens available, the packet is transmitted without delay. If there are insufficient tokens, the packet is delayed until there are enough tokens to allow transmission. Shapers do not drop frames with a small burst of traffic, but they can add latency.

The EVC Shaper Configuration mode is accessed using the **shaper** <*name*> **[**<*slot*>**]** command from the Global Configuration mode as follows:

```
(config)#shaper SHAPER1 0
(config-shaper shaper1 0)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

per interface on page 3737
rate <value> on page 3738

per interface

Use the **per interface** command to specify the interface or queue to which the Ethernet virtual connection (EVC) shaper is applied. Use the **no** form of this command to remove the shaper from the interface or queue. Variations of this command include:

per interface efm-group <*slot/group*>
per interface efm-group <*slot/group*> <*queue*>
per interface gigabit-ethernet <*slot/port*>
per interface gigabit-ethernet <*slot/port*> <*queue*>

Syntax Description

efm-group <*slot/group*>	Specifies that the shaper is applied to the Ethernet in the first mile (EFM) group.
gigabit-ethernet <*slot/port*>	Specifies that the shaper is applied to a Gigabit Ethernet interface.
<*queue*>	Optional. Specifies that the shaper is applied to an interface queue. Valid range is **0** to **7**. Separate queues in a list using commas (for example, **1,3**) or use a hyphen to define a range (for example, **1-3**).

Default Values

By default, no EVC shapers are configured.

Command History

Release R10.10.0	Command was introduced.
Release R11.1.0	Command was expanded to include the <*queue*> option.

Functional Notes

You can apply a shaper to an interface or apply a shaper to an interface queue, but you cannot do both with a single shaper. These actions are mutually exclusive.

An interface can have up to seven unique per-queue shapers and one per-interface shaper applied to it. If more than seven unique per-queue shapers are applied to an interface, they are displayed as **disabled** in the output of the **show shaper** command.

Usage Examples

The following example specifies that the EVC shaper **SHAPER1** is applied to the EFM group **1/1**:

(config)**#shaper SHAPER1 0**
(config-shaper shaper1 0)**#per interface efm-group 1/1**

The following example specifies that the EVC shaper **SHAPER1** is applied to queues **1**, **3**, **4**, and **5** on the Gigabit Ethernet interface **0/1**:

(config)**#shaper SHAPER1 0**
(config-shaper shaper1 0)**#per interface gigabit-ethernet 0/1 1, 3-5**

rate <*value*>

Use the **rate** command to configure the Ethernet virtual connection (EVC) shaper egress traffic rate. Use the **no** form of this command to return to the default shaper rate value.

Syntax Description

<*value*>	Specifies the EVC shaper rate in kilobits per second (kbps). Valid range is **0** to **1000000**.

Default Values

By default, the EVC shaper (when configured) uses a rate of **1000000** kbps.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that EVC shaper **SHAPER1** uses an egress traffic rate of **3500** kbps:

(config)**#shaper SHAPER1 0**
(config-shaper shaper1 0)**#rate 3500**

CARRIER ETHERNET TERMINAL LOOPBACK COMMAND SET

In a Carrier Ethernet terminal loopback test, traffic is sent up-stream to a remote AOS device and then looped back just prior to egressing the remote AOS unit. A flow approaching the remote device's user network interface (UNI) port interface is turned back toward the switch fabric as close as possible to the UNI interface and returns traffic to the originating AOS device that is subject the same conditioning associated with the remote device's configured egress queue management and classification rules for down-stream traffic (such as Quality of Service (QoS) policers, shapers, matching criteria, and queues). Terminal loopbacks are commonly used to validate how a remote devices perform QoS on down-stream traffic by providing insight into rate limiting functionality on configured policers, traffic prioritization in egress queues, and traffic shaping as it is looped back towards the originating device.

Because Ethernet address rules do not allow frames containing the same source MAC address to arrive from different ports on a device, the AOS unit must swap the destination and source MAC address of packets that are returned (looped back) during a terminal loopback test. The source MAC address and destination MAC addresses in the frame are swapped when the data is looped back so that the incoming source and destination addresses become the outgoing destination and source addresses, respectively.

The Carrier Ethernet Terminal Loopback command set is used to configure the parameters of a terminal loopback object.

To create a terminal loopback object and/or activate the Carrier Ethernet Terminal Loopback Configuration mode, enter the **ethernet loopback terminal** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ethernet loopback terminal TERMINAL 0
Facility loopback "TERMINAL" created
(config-eth-lbk-term TERMINAL 0)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

match on page 3740
set interface on page 3741

match

Use the **match** command to specify the traffic matching criteria used by the terminal loopback object to identify which traffic should be looped back. Packets about to egress the User Network Interface (UNI) port interface specified in the terminal loopback object will be looped back if the packet matches the criteria specified by the command. Use the **no** form of this command to remove the match criteria. Variations of this command include:

match destination mac address <*mac address*>
match destination mac address system
match single-tag s-tag <*vlan id*>

Syntax Description

destination mac address	Specifies that traffic will be looped back based on the destination MAC address. Packets just about to egress the interface specified in the terminal loopback object will be looped back if the packet's destination MAC address matches the specified MAC address.
<*mac address*>	Specifies a valid 48-bit MAC address as the destination MAC address for filtering traffic before egressing the interface. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
system	Specifies the system loopback MAC address as the destination MAC address for matching looped back traffic just prior to egressing the interface. This keyword can only be used if a system loopback MAC address has been specified. For more information on configuring the system loopback MAC address, refer to *ethernet loopback system mac address on page 1281*.
single-tag s-tag <*vlan id*>	Specifies that traffic will be looped back based on the service provider's virtual local area network (VLAN) ID. Valid <*vlan id*> range is **2** to **4094**.

Default Values

By default, all traffic on the connected UNI port interface is matched.

Command History

Release R13.7.0	Command was introduced.

Usage Examples

The following example specifies that traffic about to egress the UNI port interface should be filtered based on the destination MAC address **00:AO:C8:00:00:02**:

(config)**#ethernet loopback facility TERMINAL 0**
Facility loopback "TERMINAL" created
(config-eth-lbk-term TERMINAL 0)**#match destination mac address 00:A0:C8:00:00:02**

set interface

Use the **set interface** command to specify the User Network Interface (NNI) port interface that will loop back matching traffic. Traffic about to egress this interface will be looped back if it matches the match criteria specified in the termanl loopback object. If no match criteria is specified, all traffic egressing the interface will be looped back. Use the **no** form of this command to remove the specified association. Variations of this command include:

set interface efm-group <*slot/group*>
set interface gigabit-ethernet <*slot/port*>

Syntax Description

efm-group <*slot/group*>	Specifies an Ethernet in the first mile (EFM) group as the UNI port interface that will loop back matching traffic.
gigabit-ethernet <*slot/port*>	Specifies a Gigabit Ethernet interface as the UNI port interface that will loop back matching traffic.

Default Values

No default values are necessary for this command.

Command History

Release R13.7.0	Command was introduced.

Usage Examples

The following example specifies Gigabit Ethernet **0/1** interface as the UNI port interface that will loop back traffic:

(config)**#ethernet loopback facility TERMINAL 0**
Facility loopback “TERMINAL” created
(config-eth-lbk-term TERMINAL 0)**#set interface gigabit-ethernet 0/1**

FACILITY MAC SWAP LOOPBACK COMMAND SET

In a facility media access control (MAC) swap loopback test, traffic is looped back upon ingressing the AOS unit. A flow ingressing the Metro Ethernet network (MEN) port interface is turned back toward that interface immediately upon entering the switch fabric. This loopback incorporates only the conditioning associated with the device's MEN port (shaping). Facility loopbacks are commonly used to validate round-trip data flow between a test head and a remote device's interface to the Ethernet backhaul.

Because Ethernet address rules do not allow frames containing the same source MAC address to arrive from different ports on a device, the AOS unit must swap the destination and source MAC address of packets that are returned (looped back) during a facility MAC swap loopback test. The source MAC address and destination MAC addresses in the frame are swapped when the data is looped back so that the incoming source and destination addresses become the outgoing destination and source addresses, respectively.

The Facility MAC Swap Loopback command set is used to configure the parameters of a facility loopback object.

To create a facility loopback object and/or activate the Facility MAC Swap Loopback Configuration mode, enter the **ethernet loopback facility** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ethernet loopback facility FACILITY 0
Facility loopback "FACILITY" created
(config-eth-lbk-fac FACILITY 0)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

match on page 3743
set interface on page 3744

match

Use the **match** command to specify the traffic matching criteria used by the facility loopback object to identify which traffic should be looped back. Packets ingressing the Metro Ethernet network (MEN) port interface specified in the facility loopback object will be looped back if the packet matches the criteria specified by the command. Use the **no** form of this command to remove the match criteria. Variations of this command include:

match destination mac address <*mac address*>
match destination mac address system

Syntax Description

destination mac address	Specifies that traffic will be looped back based on the destination MAC address. Packets ingressing the interface specified in the facility loopback object will be looped back if the packet's destination MAC address matches the specified MAC address.
<*mac address*>	Specifies a valid 48-bit MAC address as the destination MAC address for filtering traffic ingressing the interface. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
system	Specifies the system loopback MAC address as the destination MAC address for matching looped back traffic ingressing the interface. This keyword can only be used if a system loopback MAC address has been specified. For more information on configuring the system loopback MAC address, refer to *ethernet loopback system mac address on page 1281*.

Default Values

By default, all traffic on the connected MEN port interface is matched.

Command History

Release R11.1.0	Command was introduced.

Usage Examples

The following example specifies that traffic ingressing the MEN port interface should be filtered based on the destination MAC address **00:AO:C8:00:00:02**:

(config)**#ethernet loopback facility FACILITY 0**
Facility loopback "FACILITY" created
(config-eth-lbk-fac FACILITY 0)**#match destination mac address 00:A0:C8:00:00:02**

set interface

Use the **set interface** command to specify the Metro Ethernet network (MEN) port interface that will loop back matching traffic. Traffic ingressing this interface will be looped back if it matches the match criteria specified in the facility loopback object. If no match criteria is specified, all traffic ingressing the interface will be looped back. Use the **no** form of this command to remove the specified association. Variations of this command include:

set interface efm-group <*slot/group*>
set interface gigabit-ethernet <*slot/port*>

Syntax Description

efm-group <*slot/group*>	Specifies an Ethernet in the first mile (EFM) group as the MEN port interface that will loop back matching traffic.
gigabit-ethernet <*slot/port*>	Specifies a Gigabit Ethernet interface as the MEN port interface that will loop back matching traffic.

Default Values

No default values are necessary for this command.

Command History

Release R11.1.0	Command was introduced.

Usage Examples

The following example specifies Gigabit Ethernet **0/1** interface as the MEN port interface that will loop back traffic:

(config)**#ethernet loopback facility FACILITY 0**
Facility loopback “FACILITY” created
(config-eth-lbk-fac FACILITY 0)**#set interface gigabit-ethernet 0/1**

SYSTEM CONTROL EVC COMMAND SET

The system control Ethernet virtual connection (EVC) command set is used to configure the system control EVC. The EVC is used to separate the session control Point-to-Point Protocol over Ethernet (PPPoE) from regular customer services on the AOS device and to provide dynamic provisioning. The EVC is linked logically to the system control virtual routing and forwarding (VRF) instance and is always present in the AOS configuration.

To enter the System Control EVC Configuration Mode, enter the **system-control-evc** from the Global Configuration mode prompt as follows:

```
(config)#system-control-evc
(config-sys-ctrl-evc)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

acfc accept-compressed on page 3747
connect men-port on page 3748
connect uni gigabit-ethernet <slot/port> on page 3749
dynamic-dns on page 3750
encap on page 3752
ip commands begin on page 3753
ipv6 commands begin on page 3782
keepalive <value> on page 3818
max-reserved-bandwidth <value> on page 3819
men-pri on page 3820
peer default ip address <ipv4 address> on page 3821
peer default ipv6 interface-id <interface id> on page 3822
ppp commands begin on page 3823
pppoe ac-name <name> on page 3833
pppoe service-name <name> on page 3834
qos-policy on page 3835
rtp quality-monitoring on page 3837
snmp trap on page 3838
snmp trap link-status on page 3839

s-tag on page 3840
traffic-shape rate <value> on page 3841
vrf forwarding <name> on page 3842

acfc accept-compressed

Use the **acfc accept-compressed** command to enable accepting header compressed frames even if compression is not negotiated. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 14.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example enables accepting compressed frames:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#acfc accept-compressed**

connect men-port

Use the **connect men-port** command to associate the Ethernet virtual connection (EVC) with a specific Metro Ethernet network (MEN) port so that traffic can flow to the MEN. Use the **no** form of this command to remove the association between this EVC and the specified EFM group. Variations of this command include:

connect men-port efm-group <*slot/group*>
connect men-port gigabit-ethernet <*slot/port*>

Syntax Description

efm-group <*slot/group*>	Specifies the Ethernet in the first mile (EFM) group to associate with the EVC. Valid group range is **1** to **1024**.
gigabit-ethernet <*slot/port*>	Specifies the Gigabit Ethernet subinterface to associate with the EVC.

Default Values

By default, no interfaces are connected to the EVC.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example associates the system control EVC with EFM group **1**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#connect men-port efm-group 1/1**

connect uni gigabit-ethernet <*slot/port*>

Use the **connect uni** command to associate the system control Ethernet virtual connection (EVC) with a user network interface (UNI). Use the **no** form of this command to remove the association between the EVC and the UNI.

Syntax Description

gigabit-ethernet <*slot/port*>	Specifies the Gigabit Ethernet subinterface to associate with the system control EVC.

Default Values

By default, the system control EVC is not associated with an interface.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example associates the system control EVC with the Gigabit Ethernet subinterface 1/1:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#connect uni gigabit-ethernet 1/1**

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#dynamic-dns dyndns-custom host user pass**

encap

Use the **encap** command to enable encapsulation mode in the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable encapsulation. Variations of this command include:

encap ethernet
encap pppoe

Syntax Description

ethernet	Specifies that the encapsulation mode of the EVC is Ethernet.
pppoe	Specifies that the encapsulation mode of the EVC is Point-to-Point Protocol over Ethernet (PPPoE).

Default Values

By default, the system control EVC encapsulation mode is set to **pppoe**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example sets the system control EVC encapsulation mode to **ethernet**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#encap ethernet**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for IPv4 packets transmitted on or received from the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group <*ipv4 acl name*> **in**
ip access-group <*ipv4 acl name*> **out**

Syntax Description

<ipv4 acl name>	Applies the named IPv4 ACL to the EVC.
in	Enables access control on IPv4 packets received on the specified interface.
out	Enables access control on IPv4 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example configures the router to only allow IPv4 Telnet traffic (as defined in the user-configured **TelnetOnly** ACL) into the system control EVC:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#system-control-evc**
(config-sys-ctrl-evc)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to the system control Ethernet virtual connection (EVC). IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an EVC.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the system control EVC:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the system control EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip access-policy PRIVATE**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii <*string*> **| hex** <*value*>**] [client-id [**<*interface*> **|** <*identifier*>**]] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp client-id [<*interface*> **|** <*identifier*>**] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp hostname *"*<*string*>*"* **[no-default-route | no-domain-name | no-nameservers] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track <*name*>**] [**<*administrative distance*>**]**
ip address dhcp track <*name*> **[**<*administrative distance*>**]**

Syntax Description

<*administrative distance*>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii <*string*>	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex <*value*>	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<*interface*>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<*identifier*>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the <*identifier*> option.
hostname <*"string"*>	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

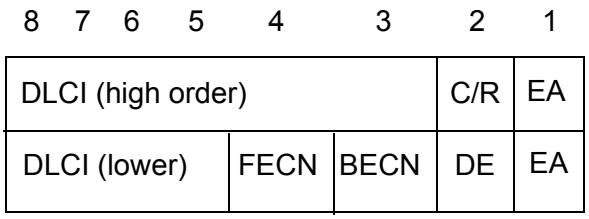
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *“<string>”* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip address dhcp hostname “adtran” no-default-route no-domain-name no-nameservers 5**

ip address negotiated

Use the **ip address negotiated** command to allow the system control Ethernet virtual connection (EVC) to negotiate (i.e., be assigned) an Internet Protocol version 4 (IPv4) address from the far-end Point-to-Point Protocol (PPP) connection. Use the **no** form of this command to disable the negotiation for an IP address. Variations of this command include:

ip address negotiated
ip address negotiated <*ipv4 address*>
ip address negotiated <*ipv4 address*> **no-default**

Syntax Description

<*ipv4 address*>	Optional. Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
no-default	Optional. Prevents the insertion of a default route. Some systems already have a default route configured and need a static route to the PPP interface to function correctly.

Default Values

By default, the EVC is not assigned an address.

Command History

Release 5.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example enables the system control EVC to negotiate an IPv4 address from the far-end connection:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip address negotiated**

The following example enables the system control EVC to negotiate an IPv4 address from the far-end connection without inserting a default route:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip address negotiated no-default**

ip address range *<start ipv4 address> <end ipv4 address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single EVC (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the system control Ethernet virtual connection (EVC) (only one primary address is allowed). Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the EVC.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 /30**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip address 192.22.72.101 /30 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove a crypto map from an interface.

> NOTE *When you apply a map to an EVC, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.*

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the EVC.

Default Values

By default, no crypto maps are assigned to an EVC.

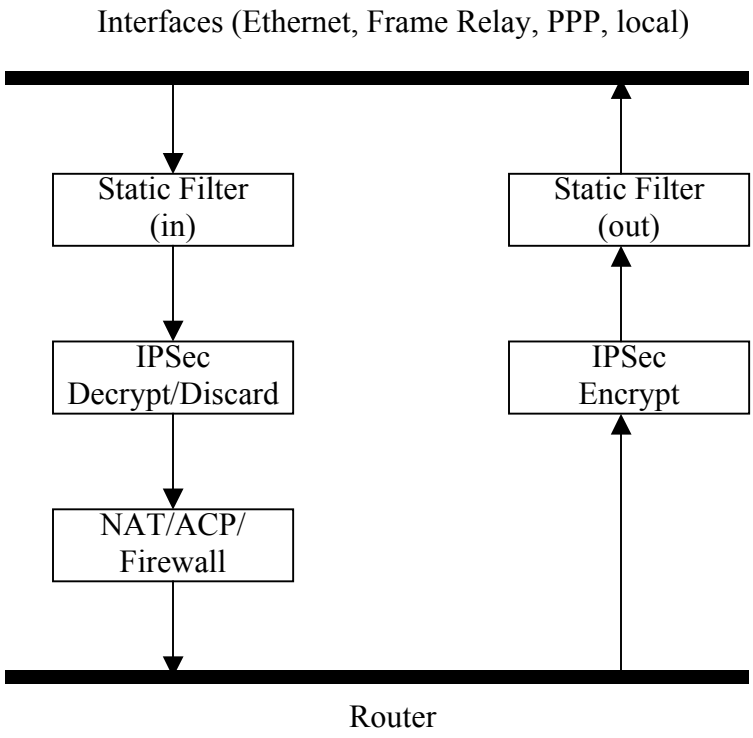
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Level Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the EVC on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an EVC. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip crypto map MyMap**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**)..

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip dhcp relay destination 192.33.4.251**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example releases the IPv4 address assigned (by DHCP) on the system control EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip dhcp release**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this EVC is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this EVC subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this EVC is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the system control EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip directed-broadcast**

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example enables traffic monitoring on the system control EVC to monitor **incoming** traffic through an ACL called **MYACL**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip flow ingress MYACL**

ip helper-address *<ipv4 address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ipv4 address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IPv4 address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248 /30 subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IPv4 address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip helper-address 192.33.5.99**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the system control Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces (all types)	1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

OSPFv2 will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip mtu 1200**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route-map to the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this EVC.

Default Values

By default, no policy route map is assigned to this EVC.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example assigns the policy route map **policy1** to the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an EVC may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip proxy-arp**

ip rip authentication

Use the **ip rip authentication** command to enable specify the Internet Protocol version 4 (IPv4) Routing Information Protocol (RIP) authentication method on the Ethernet virtual connection (EVC). Use the **no** form of this command to disable RIP authentication. Variations of this command include:

ip rip authentication key-chain <*name*>
ip rip authentication mode md5
ip rip authentication mode text

Syntax Description

key-chain <*name*>	Specifies that RIP authentication is completed using an authentication key, and specifies the key name.
mode md5	Specifies that RIP authentication is completed using message digest authentication.
mode text	Specifies that RIP authentication is completed using clear text authentication.

Default Values

By default, RIP authentication is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables RIP authentication on the EVC and specifies authentication is completed using clear text:

(config)**#system-control-evc**
(config-sys-ctrl-evc)#

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the system control Ethernet virtual connection (EVC). Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only RIP version 1 packets received on the EVC.
2	Accepts only RIP version 2 packets received on the EVC.

Default Values

By default, the EVC implements RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only accepts one version (either **1** or **2**) on an EVC.

Usage Examples

The following example configures the EVC to accept only RIP version **2** packets:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the system control Ethernet virtual connection (EVC). Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the EVC.
2	Transmits only RIP version 2 packets on the EVC.

Default Values

By default, the EVC transmit RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only transmits one version (either **1** or **2**) on an EVC.

Usage Examples

The following example configures the EVC to transmit only RIP version **2** packets:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip rip send version 2**

ip rip summary-address *<ipv4 address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable this mode.

Syntax Description

<ipv4 address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IPv4 address:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable Internet Protocol version 4 (IPv4) fast-cache switching on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an EVC requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on the EVC.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Fast switching allows an EVC to provide optimum performance when processing IPv4 traffic.

Usage Examples

The following example enables IPv4 fast switching on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip route-cache**

ip split-horizon

Use the **ip split-horizon** command to enable Internet Protocol version 4 (IPv4) Routing Information Protocol (RIP) split horizon on the Ethernet virtual connection (EVC). Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, RIP split horizon is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables RIP split horizon on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip split-horizon**

ip urlfilter *<name>*

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the system control Ethernet virtual connection (EVC) for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from the EVC. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<name>	Specifies the URL filter name to use on the EVC.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any EVCs.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** *<filter name>* **http** command before applying it to the EVC. Refer to *ip urlfilter <name> http on page 1495* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the EVC and matches the URL filter named **MyFilter**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the EVC.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the EVC.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the EVC to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the EVC.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an EVC when other unicast IPv6 addresses are not needed on the EVC. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the EVC.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the EVC:

```
(config)#system-control-evc
(config-sys-ctrl-evc)#ipv6
```


ipv6 access-group *<ipv6 acl name>*

Use the **ipv6 access-group** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to be used for IPv6 packets transmitted on or received from the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable this type of control. Variations of this command include:

ipv6 access-group *<ipv6 acl name>* **in**
ipv6 access-group *<ipv6 acl name>* **out**

Syntax Description

<ipv6 acl name>	Applies the named IPv6 ACL to the EVC.
in	Enables access control on IPv6 packets received on the EVC.
out	Enables access control on IPv6 packets transmitted on the EVC.

Default Values

By default, these commands are disabled.

Command History

Release 18.1	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Only one IPv6 ACL can be applied in each traffic direction.

Unlike in IPv4, IPv6 traffic filters include an implicit **permit** for neighbor solicitation and advertisement packets in an ACL before the traditional implicit **deny** at the end of the ACL. This prevents blocking of address resolution and unreachability detection, although this can be overridden by entering explicit **deny** commands in the IPv6 ACL.

Usage Examples

The following example applies the IPv6 ACL **Privatev6** to incoming IPv6 traffic on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 access-group Privatev6 in**

ipv6 access-policy *<ipv6 acp>*

Use the **ipv6 access-policy** command to assign a specified Internet Protocol version 6 (IPv6) access control policy (ACP) to the system control Ethernet virtual connection (EVC). IPv6 ACPs are applied to IPv6 traffic entering the EVC. Use the **no** form of this command to remove an ACP association.

Syntax Description

<ipv6 acp>	Identifies the configured IPv6 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv6 ACPs associated with the EVC.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example applies the IPv6 ACP **PRIVATEv6** to the EVC:

Enable the AOS security features:
(config)**#ipv6 firewall**

Associate the ACP with the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 access-policy PRIVATEv6**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove the IPv6 address from the EVC.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the EVC and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the EVC using the command *ipv6 address <ipv6 link-local address> link-local on page 3787*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the EVC. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the EVC.

Usage Examples

The following example adds a unicast IPv6 address to the EVC and enables IPv6 processing on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove the IPv6 address from the EVC.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the EVC and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the EVC using the command *ipv6 address <ipv6 link-local address> link-local on page 3787*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the EVC. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the EVC.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the EVC and enables IPv6 processing on the EVC:

(config)#**system-control-evc**
(config-sys-ctrl-evc)#**ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address <*ipv6 link-local address*> link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the system control Ethernet virtual connection (EVC) and enable IPv6 processing on the EVC. Use the **no** form of this command to remove the IPv6 address from the EVC.

Syntax Description

<*ipv6 link-local address*>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the EVC.

Default Values

By default, no IPv6 address is configured for the EVC and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

A single link-local address can be manually configured on an EVC. The lower 64 bits of the specified address become the Interface ID for the EVC, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the EVC and can be derived from the EVC's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the EVC.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the EVC. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the EVC.

Usage Examples

The following example manually creates a link-local IPv6 address on the EVC and enables IPv6 processing:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 address autoconfig

Use the **ipv6 address autoconfig** command to enable Internet Protocol version 6 (IPv6) processing on the system control Ethernet virtual connection (EVC), create a local-link IPv6 address for the EVC, and allow the EVC to automatically configure itself based on advertisements from other routers on the link. Use the **no** form of this command to remove all autoconfigured addresses, prefixes, and any resulting routes from the EVC and also causes the EVC to cease processing received router advertisements (RAs).Variations of this command include:

ipv6 address autoconfig
ipv6 address autoconfig default
ipv6 address autoconfig default metric <*value*>

Syntax Description

default	Optional. Specifies that the EVC maintain a list of advertising routers that are willing to be IPv6 default routers.
metric <*value*>	Optional. Specifies the administrative distance for a default router maintained in the default router list. Range is **1** to **255**. Routes with lower administrative distance are favored.

Default Values

By default, no IPv6 addresses are configured for the EVC and IPv6 processing is not enabled. When an IPv6 address is configured automatically, the administrative distance for default routers is **2** by default.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

When autoconfiguration is enabled, the EVC listens for RA messages that tell the EVC how it should be configured. The EVC then creates addresses for advertised 64-bit prefixes with the A flag in the IPv6 address set using stateless address autoconfiguration (SLAAC). The addresses use the EUI-64 interface ID in the lower 64 bits of the address. A route type of *Connected* is added to the route table if the L flag on the prefix advertisement (on-link flag) is also set.

Usage Examples

The following example enables IPv6 processing on the EVC, creates a link-local IPv6 address for the EVC, and allows the EVC to automatically configure itself for IPv6:

(config)#**system-control-evc**
(config-sys-ctrl-evc)#**ipv6 address autoconfig**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname <*partial fqdn*>
ipv6 address dhcp hostname fqdn <*fqdn*>
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 3782*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 address 2001:DB8:1::1/64**
(config-sys-ctrl-evc)**#ipv6 address dhcp fqdn client@company.com**

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*

Use the **ipv6 address named-prefix** command to create an Internet Protocol version 6 (IPv6) address for the Ethernet virtual connection (EVC) using the values in a named prefix. Use the **no** form of this command to remove the address from the EVC. Variations of this command include:

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*
ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>* **eui-64**

Syntax Description

<prefix name>	Specifies the named prefix to use to create the address.
<ipv6 address/prefix-length>	Specifies the address portion appended to the named prefix to create a 128-bit host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
eui-64	Optional. Indicates that the interface ID is to be placed in the lower 64 bits of the address.

Default Values

By default, no IPv6 addresses are specified on the EVC.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system control and system managment EVCs.

Usage Examples

The following example creates an IPv6 address on the EVC using the named prefix **PREFIX1**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 address named-prefix PREFIX1 2001:1:0:/48**

ipv6 crypto map *<name>*

Use the **ipv6 crypto map** command to associate Internet Protocol version 6 (IPv6) crypto maps with the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove a crypto map from the EVC.

Syntax Description

<name>	Specifies the IPv6 crypto map name that you wish to assign to the EVC.

Default Values

By default, no crypto maps are assigned to an EVC.

Command History

Release R10.7.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Only one IPv6 crypto map can be specified per EVC, and the crypto map is applied within the virtual routing and forwarding (VRF) instance to which the EVC belongs. To apply the IPv6 crypto map, the EVC must have IPv6 enabled. In addition, the EVC must have an IPv6 address of appropriate scope to allow connectivity to peer's addresses as specified in the crypto map's entries.

Usage Examples

The following example applies all IPv6 crypto maps with the name **MyMap** to the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6**
(config-sys-ctrl-evc)**#ipv6 crypto map MyMap**

ipv6 dhcp client information refresh minimum <*seconds*>

Use the **ipv6 dhcp client information refresh minimum** command to specify the minimum value the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the system control Ethernet virtual connection (EVC) accepts as its information refresh timer. Use the **no** version of this command to return to the default setting.

Syntax Description

<*seconds*>	Specifies the refresh timer in seconds. Valid range is **600** to **3600** seconds.

Default Values

By default, the DHCPv6 client refresh timer is set to **600** seconds.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example specifies the DHCPv6 client refresh timer for the EVC is **800** seconds:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 dhcp client information refresh minimum 600**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#system-control-evc**
(config-syst-ctrl-evc)**#ipv6 dhcp client pd PREFIX1**

ipv6 dhcp relay destination *<ipv6 address>*

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the system control Ethernet virtual connection (EVC). Variations of this command include:

ipv6 dhcp relay destination *<ipv6 address>*
ipv6 dhcp relay destination *<ipv6 address>* *<interface>*
ipv6 dhcp relay destination *<ipv6 address>* **system-control-evc**
ipv6 dhcp relay destination *<ipv6 address>* **system-management-evc**

Syntax Description

<ipv6 address>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** *<ipv6 address>* **?** to display a list of valid interfaces.
system-control-evc	Optional. Specifies the output interface for sending messages to the DHCPv6 server is the system control EVC.
system-management-evc	Optional. Specifies the output interface for sending messages to the DHCPv6 server is the system management EVC.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

To configure an EVC to function as a DHCPv6 relay agent, you must first enable IPv6 on the EVC using the command *ipv6 on page 3782*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6**
(config-sys-ctrl-evc)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped mulitcast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the system control Ethernet virtual connection (EVC) and specify that the EVC is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the EVC, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the EVC. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this EVC. All DHCPV^ requests received on this EVC are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the EVC.

Command History

Release R10.1.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Enabling the EVC as a DHCPv6 server using this command places the EVC into DHCPv6 server mode. DHCPv6 modes (server, client, or relay) are mutually exclusive at the EVC. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the EVC as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 address 2001:DB8:1::1/64**
(config-sys-ctrl-evc)**#ipv6 dhcp server POOL1**

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the system control Ethernet virtual connection (EVC) in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the EVC.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the EVC in host mode:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 mode host unicast**

ipv6 mtu *<size>*

Use the **ipv6 mtu** command to specify the maximum transmission unit (MTU) for Internet Protocol version 6 (IPv6) packets on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Specifies the MTU value. Valid range is **1280** to **1500** bytes.

Default Values

By default, the MTU of the EVC is set to **1280** bytes.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

In IPv6, the minimum MTU is 1280 octets. Any link that has an MTU less than 1280 octets must use link fragmentation and reassembly that is transparent to IPv6 (for example, the Fragmentation Header). Sources in the IPv6 network are expected to perform path maximum transmission unit (PMTU) discovery to send packets larger than 1280 octets. PMTU works in the following manner: First, the sending node assumes the link MTU of the interface from which the traffic is being forwarded and then sends the IPv6 packet at the link MTU size. If a router on the path is unable to forward the packet, it sends an ICMP *Packet Too Big* message back to the sending node containing the link MTU of the link on which the packet forwarding failed. The sending node then rests the PMTU to the value of the MTU field in the Internet Control Message Protocol version 6 (ICMPv6) *Packet Too Big* message, and the packet is resent.

The MTU for IPv6 packets can be set on a per-EVC basis. There are two methods for setting MTUs for EVCs if required: one for Layer 3 EVCs, and one for the underlying Layer 1 and Layer 2 EVCs. For all EVC types, use the **ipv6 mtu** *<size>* command to specify the IPv6 MTU in bytes from the EVC's configuration mode. The minimum MTU setting for IPv6 is **1280** bytes, and the maximum is **1500** bytes. The IPv6 MTU value is independent of the IPv4 MTU setting (set with the command *ip mtu <size> on page 3771*).

When the EVC is forwarding the IPv6 packet as a router, if the packet size exceeds the IPv6 MTU of the egress EVC, the packet is dropped and ICMPv6 *Packet Too Big* message is sent to the source. When originating an IPv6 packet from the local IPv6 stack, and the packet is larger than the IPv6 MTU of the egress EVC, the packet is fragmented and sent.

Usage Examples

The following example specifies the IPv6 MTU value for the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 mtu 1350**

ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** command to specify that the Advertisement Interval Option is sent in Internet Protocol version 6 (IPv6) router advertisement (RA) messages from the router. This command is effectual only when the system control Ethernet virtual connection (EVC) is in router mode. Use the **no** form of this command to return to the default interval.

Syntax Description

No subcommands.

Default Values

By default, Advertisement Interval Options are not sent in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Sending the Advertisement Interval Option should be enabled when the router is functioning in a mobile IP environment to aid movement detection by mobile nodes. This option contains the current value of the maximum router advertisement interval configured using the command *ipv6 nd ra interval on page 3812*.

Usage Examples

The following example specifies that the EVC include Advertisement Interval Options in RA messages sent from the router:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd advertisement-interval**

ipv6 nd cache max-incomplete <*number*>

Use the **ipv6 nd cache max-incomplete** command to specify the maximum number of incomplete entries the Neighbor Discovery (ND) cache retains. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of incomplete ND entries to retain in the cache. Valid range is **1** to **321**.

Default Values

By default, the incomplete ND entries can take at maximum one-third of the possible ND cache entries (varies by product).

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example specifies that the interface stores **150** incomplete entries in the ND cache:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd cache max-incomplete 150**

ipv6 nd dad attempts *<number>*

Use the **ipv6 nd dad attempts** command to specify the number of neighbor solicitation (NS) messages sent by the system control Ethernet virtual connection (EVC) when performing Internet Protocol version 6 (IPv6) duplicate address detection (DAD). This command is effectual when the EVC is in either host or router mode. Use the **no** form of this command to return to the default value.

Syntax Description

<number>	Specifies the number of NS messages that will be sent. Range is **0** to **10** messages. A value of **0** disables DAD on the interface.

Default Values

By default, the EVC sends **1** NS message.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

DAD is used by devices to determine if IPv6 addresses are unique before they are applied to EVCs. DAD is used in NS messages to detect duplicate unicast addresses. The Target Address fields in the NS messages are set to the IPv6 address for which duplication is being detected. Destination IPv6 addresses for DAD in NS messages are the solicited-node multicast version of the address being tested. Source IPv6 addresses for DAD are set to the IPv6 unspecified address (::). Once the IPv6 address is determined by DAD to be unique, it can be applied to the EVC on the node.

DAD in AOS is performed when an EVC transitions state from DOWN to UP or when manually configuring an address. When performing DAD because of an interface transition, DAD will happen immediately after the EVC transition and again 40 seconds later to cooperate with the port being connected to an Ethernet switch.

Usage Examples

The following example specifies that **3** NS messages are sent by the EVC when performing DAD:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd dad attempts 3**

ipv6 nd generate-packet

Use the **ipv6 nd generate-packet** command to generate and send test packets from the Ethernet virtual connection (EVC) for Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages. Use the **no** form of this command to disable packet generation. Variations of this command include:

ipv6 nd generate-packet neighbor-advertisement <*source ipv6 address*> <*destination ipv6 address*> <*Layer 2 address*>
ipv6 nd generate-packet neighbor-solicitation <*source ipv6 address*> <*destination ipv6 address*> <*target ipv6 address*>
ipv6 nd generate-packet router-advertisement

Syntax Description

neighbor-advertisement	Specifies that test packets are generated for neighbor advertisement (NA) messages.
neighbor-solicitation	Specifies that test packets are generated for neighbor solicitation (NS) messages.
router-advertisement	Specifies that test packets are generated for router advertisement (RA) messages.
<*source ipv6 address*>	Specifies the source address of the test packet. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*destination ipv6 address*>	Specifies the destination address of the test packet. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*Layer 2 address*>	Specifies the Layer 2 destination address for the test packet using a medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**) or 0xABCDEF format (for example, **1x234567**).
<*target ipv6 address*>	Specifies the IPv6 address of the target neighbor for NS test packets. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

Default Values

By default, test packets are not generated for ND messages.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example generates test packets for RA messages on the EVC:

(config)**#system-control-evc**
(config-system-cntrl-evc)**#ipv6 nd generate-packet router-advertisement**

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command to specify the M flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. The M flag instructs hosts receiving the RA that they can use stateful Dynamic Host Configuration Protocol version 6 (DHCPv6) to configure addresses and nonaddress information. Use the **no** form of this command to disable the setting of the M flag.

Syntax Description

No subcommands.

Default Values

By default, the M flag is not set in RAs.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Functional Notes

If you specify that the M flag is set in RA messages, you do not need to set the 0 flag (it becomes redundant).

Usage Examples

The following example sets the M flag for RA messages sent by the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd managed-config-flag**

ipv6 nd ns-interval *<value>*

Use the **ipv6 nd ns-interval** command to specify the interval between transmission of certain Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages and to control what ND value is advertised in router advertisement (RA) messages. This command is effectual whether the system control Ethernet virtual connection (EVC) is in host or router mode. Use the **no** form of this command to return the interval to the default value.

Syntax Description

<value>	Specifies the time (in milliseconds) between neighbor message transmissions. Valid range is **1000** to **3600000** ms.

Default Values

By default, the interval is set to **1000** ms for internal use by the router and **0** (unspecified) is sent in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

This command controls the spacing of neighbor solicitation (NS) messages for functions such as address resolution, reachability detection, and duplicate address detection (DAD). For DAD it also serves as the amount of time after the last transmission before the detection phase of autoconfiguration terminates. In addition, the command controls the interval between unsolicited neighbor advertisement (NA) messages.

Usage Examples

The following example changes the interval between RA messages sent from the EVC to **2000** ms:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd ns-interval 2000**

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command to specify the O flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the system control Ethernet virtual connection (EVC) is in router mode. When the O flag is set, hosts receiving the RA messages are instructed that they may use stateless Dynamic Host Configuration Protocol version 6 (DHCPv6) to receive information that is not IPv6 addressing information, and to use some other method (whether through manual configuration, stateless address autoconfiguration (SLAAC), etc.) for addressing information. Use the **no** form of this command to disable the O flag setting.

Syntax Description

No subcommands.

Default Values

By default, the O flag is not set in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

If the M flag is set for RA messages, you do not need to set the O flag.

Usage Examples

The following example sets the O flag in RA messages from the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd other-config-flag**

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove the specified prefix configuration from the EVC. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the EVC's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the EVC is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the EVC. Prefixes for IPv6 addresses configured on a router EVC are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the EVC.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the EVC's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ipv6 nd purge-timer <*value*>

Use the **ipv6 nd purge-timer** command to specify the maximum amount of time an unused Internet Protocol version 6 (IPv6) neighbor entry remains in the neighbor cache. This command is effectual for the system control Ethernet virtual connection (EVC) in either host or router mode. Use the **no** form of this command to return the purging interval to the default value.

Syntax Description

<*value*>	Specifies the neighbor cache entry storage time in minutes. Valid range is **10** to **1440** minutes.

Default Values

By default, idle (STALE) neighbor cache entries are cleared after **1440** minutes (24 hours).

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

This command applies to EVCs in either router or host mode. A neighbor entry is typically purged when neighbor unreachability detection (NUD) is invoked and the neighbor is determined to no longer be reachable. However, NUD is not performed on idle (STALE) neighbor entries, so this command provides a method for purging unused entries after a specified amount of time.

Usage Examples

The following example specifies that idle neighbor entries in the neighbor cache are removed after **800** minutes:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd purge-timer 800**

ipv6 nd ra interval

Use the **ipv6 nd ra interval** command to specify the interval between transmission of Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the system control Ethernet virtual connection (EVC) is in router mode. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 nd ra interval *<max time>*
ipv6 nd ra interval *<max time> <min time>*
ipv6 nd ra interval msec *<max time>*
ipv6 nd ra interval msec *<max time> <min time>*

Syntax Description

<max time>	Specifies the maximum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **4** to **1800** seconds and **70** to **1800000** ms.
<min time>	Optional. Specifies the minimum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **3** seconds to 75 percent of the configured maximum time value in seconds, or **30** ms to 75 percent of the configured maximum time value in ms.
msec	Optional. Specifies that the time values are in milliseconds.

Default Values

By default, the interval is set in seconds and has a maximum interval time of **200** seconds and a minimum interval time of 75 percent of the maximum seconds value, but not less than **3** seconds.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

If this router is used as a default router, the interval between RA messages should not be set to a larger value than the RA lifetime set by the command *ipv6 nd ra lifetime <value> on page 3813*, which has a default value of **1800** seconds.

Usage Examples

The following example specifies that the maximum interval in seconds between RA message transmissions is **300**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd ra interval 300**

ipv6 nd ra lifetime <*value*>

Use the **ipv6 nd ra lifetime** command to specify the router lifetime advertised in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the system control Ethernet virtual connection (EVC) is in router mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

ipv6 nd ra lifetime <*value*>
ipv6 nd ra lifetime default-route

Syntax Description

<*value*>	Specifies the router lifetime in seconds. Range is **0** to **9000** seconds. A value of **0** indicates this is not a default router. A value other than 0 indicates to other nodes that this router can be used as a default router.
default-route	Specifies the RA lifetime is **0** if no default route exists on any IPv6 interface.

Default Values

By default, the router lifetime is set to **1800** seconds.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.
Release R11.5.0	Command was expanded to include the **default-route** parameter.

Functional Notes

A value other than **0** for a router lifetime should be larger than the router advertisement interval specified in the command *ipv6 nd ra interval on page 3812*.

Usage Examples

In the following example, the router lifetime advertised in RA messages is **3000** seconds:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd ra lifetime 3000**

ipv6 nd ra reachable-time *<value>*

Use the **ipv6 nd ra reachable-time** command to specify the value advertised for reachable time in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command also specifies the internal base reachable time used by the router. This command is effectual for the system control Ethernet virtual connection (EVC) in either host or router mode. Use the **no** form of this command to return the reachability value to the default setting.

Syntax Description

<value>	Specifies the reachability time in milliseconds. Range is **0** to **3600000** ms. A value of **0** indicates the reachable time is unspecified.

Default Values

By default, the router advertises a reachability time of **0** ms and uses an internal value of **30000** ms.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

This command is effectual for EVCs in either router or host mode. For hosts, this value sets the internal reachable time used by the host if no RAs are received specifying a different value. For routers, the value indicates the amount of time a device is considered reachable after having received a reachability confirmation in neighbor unreachabililty detection (NUD).

Usage Examples

The following example specifies that a reachability time of **50000** ms is advertised in RA messages:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd ra reachable-time 50000**

ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command to specify whether Internet Protocol version 6 (IPv6) router advertisement (RA) messages will be suppressed. This command is only effectual when the system control Ethernet virtual connection (EVC) is in router mode. Use the **no** form of this command to begin sending RA messages.

Syntax Description

No subcommands.

Default Values

By default, RA messages are not suppressed. When IPv6 routing is not enabled on the router, or when implemented in a host-only mode, the default setting is to suppress advertisements on all EVC types.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example suppresses RA messages on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd ra suppress**

ipv6 nd router-preference

Use the **ipv6 nd router-preference** command to specify the default router preference value set in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. Setting this preference helps the receivers of RA messages to determine the preference of one router over another as a default router in environments with multiple routers. Use the **no** form of this command to return the preference to the default setting. Variations of this command include:

ipv6 nd router-preference high
ipv6 nd router-preference low
ipv6 nd router-preference medium

Syntax Description

high	Specifies the preference value is high.
low	Specifies the preference value is low.
medium	Specifies the preference value is medium.

Default Values

By default, the router preference is set to medium.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example specifies that the advertised default router preference is high:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 nd router-preference high**

ipv6 route-cache

Use the **ipv6 route-cache** command to enable Internet Protocol version 6 (IPv6) fast-cache switching on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 18.2	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

Fast switching allows an EVC to provide optimum performance when processing IPv6 traffic.

Usage Examples

The following example enables IPv6 fast switching on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ipv6 route-cache**

keepalive *<value>*

Use the **keepalive** command to enable the transmission of keepalive packets on the system control Ethernet virtual connection (EVC) and specify the time interval in seconds between transmitted packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Defines the time interval (in seconds) between transmitted keepalive packets. Valid range is **0** to **32767** seconds.

Default Values

By default, the time interval between transmitted keepalive packets is **10** seconds.

Command History

Release 1.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

If three keepalive packets are sent to an EVC with no response, the EVC is considered down. To detect EVC failures quickly, specify a smaller keepalive time.

Usage Examples

The following example specifies a keepalive time of **5** seconds on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#keepalive 5**

max-reserved-bandwidth <*value*>

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<*value*>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.
elease 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.
Release R11.1.0	Command was expanded to include the system control Ethernet virtual connection (EVC) and system management EVC.

Usage Examples

The following example specifies **85** percent of the bandwidth on the system control EVC be available for use in user-defined queues:

(config)**#system-control-evc**
(config-sys-cntrl-evc)**#max-reserved-bandwidth 85**

men-pri

Use the **men-pri** command to specify the default value of the S-tag used in the system control Ethernet virtual connection (EVC) communication. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-pri inherit
men-pri <*value*>

Syntax Description

inherit	Specifies that the S-tag priority value is inherited from the customer equipment (CE) virtual local area network (VLAN).
<*value*>	Specifies a priority value for the S-tag. Valid range is **0** to **7**.

Default Values

By default, the S-tag is set to **inherit**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that the S-tag has a priority of **5** on the EVC:

(config)#**system-control-evc**
(config-sys-ctrl-evc)#**men-pri 5**

peer default ip address *<ipv4 address>*

Use the **peer default ip address** command to specify the default peer Internet Protocol version 4 (IPv4) address of the remote end of the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove an assigned IPv4 address.

Syntax Description

<ipv4 address>	Specifies the default peer IPv4 address for the remote end. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there is no assigned default peer IPv4 address.

Command History

Release 3.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

This command is useful if the peer does not send the IPv4 address option during Point-to-Point Protocol (PPP) negotiations.

Usage Examples

The following example sets the default peer IPv4 address to **192.22.71.50**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#peer default ip address 192.22.71.50**

peer default ipv6 interface-id *<interface id>*

Use the **peer default ipv6 interface-id** command to specify the default peer Internet Protocol version 6 (IPv6) interface ID of the remote end of the system control Ethernet virtual connection (EVC). Use the **no** form of this command to remove an assigned IPv6 interface ID.

Syntax Description

<interface id>	Specifies the default peer IPv6 interface ID for the remote end. IPv6 interface IDs should be expressed in colon hexadecimal notation (**X:X:X:X**). For example, **2AA:FF:FE3F:2A1C**.

Default Values

By default, there is no assigned default peer IPv6 interface ID.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example sets the default peer IPv6 interface ID to **2AA:FF:FE3F:2A1C**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#peer default ipv6 interface-id 2AA:FF:FE3F:2A1C**

ppp authentication

Use the **ppp authentication** command to specify the authentication protocol on the system control Ethernet virtual connection (EVC) that the peer should use to authenticate itself. Use the **no** form of this command to disable this feature. Variations of this command include:

ppp authentication chap
ppp authentication pap

Syntax Description

chap	Configures Challenge-Handshake Authentication Protocol (CHAP) on the interface.
pap	Configures Password Authentication Protocol (PAP) on the interface.

Default Values

By default, PPP endpoints have no authentication configured.

Command History

Release 1.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Technology Review

CHAP and PAP are two authentication methods that enjoy widespread support. Both methods are included in AOS and are easily configured.

The authentication method set up on the local router can be different from that on the peer. Also, just because one router requires authentication from its peer does not mean it also has to authenticate itself to the peer.

Defining PAP

PAP is used to verify that the PPP peer is a permitted device by checking a user name and password configured on the peer. The user name and password are both sent unencrypted across the connecting private circuit.

PAP requires two-way message passing. First, the router that is required to be authenticated (for example, the peer) sends an authentication request with its user name and password to the router requiring authentication (for example, the local router). The local router then looks up the user name and password in the user name database within the system control EVC, and if they match sends an authentication acknowledge back to the peer.

The PPP user name and password database is separate and distinct from the global user name password database. For PAP and CHAP, use the database under the EVC configuration.

Several example scenarios are given below for clarity.

Configuring PAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (host name **Local**):

Local(config-sys-ctrl-evc)**#ppp authentication pap**
Local(config-sys-ctrl-evc)**#username farend password far**

On the peer (host name **Peer**):

Peer(config-sys-ctrl-evc)**#ppp pap sent-username farend password far**

The first line of the configuration sets the authentication mode as PAP. This means the peer is required to authenticate itself to the local router via PAP. The second line is the user name and password expected to be sent from the peer. On the peer, the **ppp pap sent-username** command is used to specify the appropriate matching user name and password.

Configuring PAP Example 2: Both routers require the peer to authenticate itself.

On the local router (host name **Local**):

Local(config-sys-ctrl-evc)**#ppp authentication pap**
Local(config-sys-ctrl-evc)**#username farend password far**
Local(config-sys-ctrl-evc)**#ppp pap sent-username nearend password near**

On the peer (host name **Peer**):

Peer(config-sys-ctrl-evc)**#ppp authentication pap**
Peer(config-sys-ctrl-evc)**#username nearend password near**
Peer(config-sys-ctrl-evc)**#ppp pap sent-username farend password far**

Now both routers send the authentication request, verify that the user name and password sent match what is expected in the database, and send an authentication acknowledge.

Defining CHAP

CHAP is a three-way authentication protocol composed of a challenge response and success or failure. The message digest 5 (MD5) protocol is used to protect user names and passwords in the response.

First, the local router (requiring its peer to be authenticated) sends a challenge containing the unencrypted user name of the peer and a random number. The user name of the peer is found in the user name database within the system control EVC of the local router. The peer then looks up the user name in the user name database within the EVC, and if found takes the corresponding password and its own host name and sends a response back to the local router. This data is encrypted. The local router verifies that the user name and password are in its own user name database within the EVC, and if so sends a success back to the peer.

The PPP user name and password database is separate and distinct from the global user name password database. For PAP and CHAP, use the database under the EVC configuration.

Several example scenarios are given below for clarity.

Configuring CHAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (host name **Local**):

Local(config-sys-ctrl-evc)**#ppp authentication chap**
Local(config-sys-ctrl-evc)**#username Peer password same**

On the peer (host name **Peer**):

Peer(config-sys-ctrl-evc)**#ppp chap password same**

The first line of this configuration sets the authentication mode to CHAP. This means the peer is required to authenticate itself to the local router via CHAP. The second line is the user name and password expected to be sent from the peer. The peer uses its **hostname** and **ppp chap password** commands to send the proper authentication information.

Both ends must have identical passwords.

Configuring CHAP Example 2: Using the ppp chap hostname command as an alternate solution.

On the local router (host name **Local**):

Local(config-sys-ctrl-evc)**#ppp authentication chap**
Local(config-sys-ctrl-evc)**#username farend password same**

On the peer (host name **Peer**):

Peer(config-sys-ctrl-evc)**#ppp chap hostname farend**
Peer(config-sys-ctrl-evc)**#ppp chap password same**

Notice the local router is expecting user name **farend** even though the peer router's host name is **Peer**. Therefore, the peer router can use the **ppp chap hostname** command to send the correct name in the challenge.

Both ends must have identical passwords.

Configuring CHAP Example 3: Both routers require each other to authenticate themselves using the same shared password.

On the local router (host name **Local**):

Local(config-sys-ctrl-evc)**#ppp authentication chap**
Local(config-sys-ctrl-evc)**#username Peer password same**

On the peer (host name **Peer**):

Peer(config-sys-ctrl-evc)**#ppp authentication chap**
Peer(config-sys-ctrl-evc)**#username Local password same**

This is basically identical to Example 1 except that both routers will now challenge each other and respond.

Both ends must have identical passwords.

Configuring CHAP Example 4: Both routers require each other to authenticate themselves using two separate shared passwords.

On the local router (host name **Local**):

Local(config-sys-ctrl-evc)**#ppp authentication chap**
Local(config-sys-ctrl-evc)**#username Peer password far**
Local(config-sys-ctrl-evc)**#ppp chap password near**

On the peer (host name **Peer**):

Peer(config-sys-ctrl-evc)**#ppp authentication chap**
Peer(config-sys-ctrl-evc)**#username Local password near**
Peer(config-sys-ctrl-evc)**#ppp chap password far**

This is basically identical to Example 3, except that there are two separate shared passwords.

Notice this example has both ends using different sets of passwords.

ppp bcp tagged-frame

Use the **ppp bcp tagged-frame** command to allow negotiation of IEEE 802.1Q-tagged packets over Bridging Control Protocol (BCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 14.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example configures the EVC to negotiate tagged frames over BCP:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ppp bcp tagged-frame**

ppp chap hostname *<name>*

Use the **ppp chap hostname** command to configure an alternate host name for Challenge-Handshake Authentication Protocol (CHAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured host name. For more information on Password Authentication Protocol (PAP) and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication on page 3823*.

Syntax Description

<name>	Specifies a host name using an alphanumeric string up to 80 characters in length.

Default Values

By default, there are no configured PPP CHAP host names.

Command History

Release 1.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example specifies a PPP CHAP host name of **my_host**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ppp chap hostname my_host**

ppp chap password *<password>*

Use the **ppp chap password** command to configure an alternate password when the peer requires Challenge-Handshake Authentication Protocol (CHAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured password. For more information on Password Authentication Protocol (PAP) and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication on page 3823*.

Syntax Description

<password>	Specifies a password using an alphanumeric string up to 80 characters in length.

Default Values

By default, there is no defined PPP CHAP password.

Command History

Release 1.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example specifies a PPP CHAP password of **my_password**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ppp chap password my_password**

ppp mtu *<size>*

Use the **ppp mtu** command to configure the Point-to-Point Protocol (PPP) maximum transmission unit (MTU) size for the system control Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Configures the window size for transmitted packets. The valid range is **64** to **2100** bytes.

Default Values

By default, the PPP MTU on an EVC is set to **1500** bytes.

Command History

Release 17.9	Command was introduced.
Release R10.10.0	Command was expanded to include the system control EVC.

Usage Examples

The following example specifies a PPP MTU of **1200** on the EVC:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ppp mtu 1200**

ppp multilink

Use the **ppp multilink** command to enable Multilink Point-to-Point Protocol (MLPPP) operation on the system control Ethernet virtual connection (EVC). Use the **no** form of this command to disable this feature. Variations of this command include:

ppp multilink fragmentation
ppp multilink interleave
ppp multilink maximum <*number*>

Syntax Description

fragmentation	Enables multilink fragmentation operation.
interleave	Enables multilink interleave operation.
maximum <*number*>	Specifies the maximum number of links allowed in a PPP multilink bundle.

Default Values

By default, MLPPP is disabled.

Command History

Release 7.1	Command was introduced.
Release 7.2	Fragmentation and interleave operation were added.
Release 11.1	Command was expanded to include the demand interface.
Release R10.10.0	Command was expanded to include the system control EVC.

Functional Notes

When enabled, the EVC is capable of the following:

- Combining multiple physical links into one logical link.
- Receiving upper layer protocol data units (PDUs), fragmenting and transmitting over the physical links.
- Receiving fragments over the physical links and reassembling them into PDUs.

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

The multilink bundle will remain active with a minimum of one physical link. Physical links may be dynamically added or removed from the multilink bundle with minor interruption to traffic flow.

Usage Examples

The following example enables MLPPP:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#ppp multilink**

ppp pap sent-username <*username*> password <*password*>

Use the **ppp pap sent-username password** command to configure a user name and password when the peer requires Password Authentication Protocol (PAP) Point-to-Point Protocol (PPP) authentication. Use the **no** form of this command to remove a configured password. For more information on PAP and Challenge-Handshake Authentication Protocol (CHAP) functionality, refer to the *Technology Review* section for the command *ppp authentication on page 3823*.

Syntax Description

<username>	Specifies a user name by alphanumeric string up to 80 characters in length (the user name is case sensitive).
<password>	Specifies a password by alphanumeric string up to 80 characters in length (the password is case sensitive).

Default Values

By default, there is no defined **ppp pap sent-username** and **password**.

Command History

Release 1.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example specifies a PPP PAP sent user name of **local** and a password of **my_password**:

```
(config)#system-control-evc
(config-sys-ctrl-evc)#ppp pap sent-username local password my_password
```


pppoe ac-name *<name>*

Use the **pppoe ac-name** command to identify the access controller (AC) with which AOS expects to establish a Point-to-Point Protocol over Ethernet (PPPoE) session. Use the **no** form of this command to return to the default setting.

Syntax Description

<name>	Specifies an AC by text string (up to 255 characters) corresponding to the AC-Name Tag under RFC 2516. If this field is not specified, any AC is acceptable. The AC value may be a combination of trademark, model, and serial ID information (or simply the medium access control (MAC) address of the unit).

Default Values

By default, no AC is specified.

Command History

Release 5.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example identifies the AC with which AOS expects to establish a PPPoE session:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#pppoe ac-name Access_Controller_Name**

pppoe service-name <*name*>

Use the **pppoe service-name** command to use this tag value to filter Point-to-Point Protocol over Ethernet (PPPoE) session offers from PPPoE servers. Use the **no** form of this command to return to the default setting.

Syntax Description

<*name*>	Specifies a service name by text string (up to 255 characters) corresponding to the Service-Name Tags under RFC 2516. This string indicates an Internet service provider (ISP) name (or a class of service (CoS) or quality of service (QoS)). If this field is not specified, any service is acceptable.

Default Values

By default, no names are specified.

Command History

Release 5.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system control Ethernet virtual connection (EVC).

Usage Examples

The following example defines a service type that is not to be accepted by AOS:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#pppoe service-name Service_Name**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in <*name*>
qos-policy out <*name*>

Syntax Description

<*name*>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the system control Ethernet virtual connection (EVC) and system management EVC.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair queue to use weighted fair queuing.
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the system control EVC:

(config)#**system-control-evc**
(config-sys-cntrl-evc)#**qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.2.0	Command was expanded to include the system control Ethernet virtual connection (EVC) and system management EVC.

Usage Examples

The following example enables RTP quality monitoring on the system control EVC:

(config)**#system-control-evc**
(config-sys-cntrl-evc)**#rtp quality-monitoring**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Us the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Usage Examples

The following example enables SNMP capability on the system control EVC:

(config)**#system-control-evc**
(config-sys-cntrl-evc)**#snmp trap**

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the system control EVC:

(config)**#system-control-evc**
(config-sys-cntrl-evc)**#no snmp trap link-status**

s-tag

Use the **s-tag** command to specify the virtual local area network (VLAN) ID used by the service provider in the system control Ethernet virtual connection (EVC) to identify traffic in the control LAN. This VLAN ID, the s-tag, is used by the carrier to mark outbound traffic from this EVC in the Metro Ethernet network (MEN). Use the **no** form of this command to return the s-tag value to the default. Variations of this command include:

s-tag *<vlan id>*
s-tag none

Syntax Description

<vlan id>	Specifies ID of the service provider VLAN. Valid range is **1** to **4094**.
none	Specifies no S-tag is used.

Default Values

By default, the s-tag is **0**, which indicates the traffic on the EVC is untagged.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the **none** parameter and the system control EVC.

Usage Examples

The following example specifies the s-tag for traffic outbound on the EVC is **20**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#s-tag 20**

traffic-shape rate <*value*>

Use the **traffic-shape rate** command to specify and enforce an output bandwidth for the system control Ethernet virtual connection (EVC). Variations of this command include:

traffic-shape rate <*value*>
traffic-shape rate <*value*> **count-eth-overhead**
traffic-shape rate <*value*> <*burst*>
traffic-shape rate <*value*> <*burst*> **count-eth-overhead**

Syntax Description

<*value*>	Specifies the rate (in bits per second) at which the interface should be shaped.
<*burst*>	Optional. Specifies the allowed burst in bytes. By default, the burst is specified as the rate divided by 5 and represents the number of bytes that would flow within 200 ms.
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.

Default Values

By default, traffic-shaping rate is disabled.

Command History

Release 10.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the **count-eth-overhead** parameter, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

Traffic shaping can be used to limit an Ethernet segment to a particular rate or to specify use of quality of service (QoS) on Ethernet or VLAN interfaces.

Usage Examples

The following example sets the outbound rate of traffic on the system control EVC to 128 kbps:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#traffic-shape rate 128000**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an Ethernet virtual connection (EVC) to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the EVC from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an EVC's VRF association will clear all IP-related settings on that EVC.

Syntax Description

<*name*>	Specifies the name of the VRF to which to assign the EVC.

Default Values

By default, EVCs are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.

Functional Notes

VRF instances must be created first before an EVC can be assigned. An EVC can only be assigned to one VRF, but multiple EVCs can be assigned to the same VRF.

An EVC will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the system control EVC to the VRF instance named **RED**:

(config)**#system-control-evc**
(config-sys-ctrl-evc)**#vrf forwarding RED**

SYSTEM MANAGEMENT EVC COMMAND SET

The system management Ethernet virtual connection (EVC) command set is used to provide an inband IP network interface for system management and control. It allows local IP address information to be provisioned and configures the underlying hardware to forward packets to the CPU for local IP stack processing. The EVC is linked logically to the system control virtual routing and forwarding (VRF) instance and is always present in the AOS configuration.

To enter the System Management EVC Configuration Mode, enter the **system-management-evc** command from the Global Configuration mode prompt as follows:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

connect men-port

Use the **connect men-port** command to associate the Ethernet virtual connection (EVC) with a specific Metro Ethernet network (MEN) port so that traffic can flow to the MEN. Use the **no** form of this command to remove the association between this EVC and the specified EFM group. Variations of this command include:

connect men-port efm-group <*slot/group*>
connect men-port gigabit-ethernet <*slot/port*>

Syntax Description

efm-group <*slot/group*>	Specifies the Ethernet in the first mile (EFM) group to associate with the EVC. Valid group range is **1** to **1024**.
gigabit-ethernet <*slot/port*>	Specifies the Gigabit Ethernet subinterface to associate with the EVC.

Default Values

By default, no interfaces are connected to the EVC.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example associates the system management EVC with EFM group **1**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#connect men-port efm-group 1/1**

connect uni gigabit-ethernet <*slot/port*>

Use the **connect uni** command to associate the system management Ethernet virtual connection (EVC) with a user network interface (UNI). Use the **no** form of this command to remove the association between the EVC and the UNI.

Syntax Description

gigabit-ethernet <*slot/port*>	Specifies the Gigabit Ethernet subinterface to associate with the system control EVC.

Default Values

By default, the system control EVC is not associated with an interface.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example associates the system management EVC with the Gigabit Ethernet subinterface 1/1:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#connect uni gigabit-ethernet 1/1
```

dynamic-dns

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org). Use the **no** form of this command to disable this feature. Variations of this command include:

dynamic-dns custom <*hostname*> <*minutes*>
dynamic-dns dyndns <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-custom <*hostname*> <*username*> <*password*>
dynamic-dns dyndns-static <*hostname*> <*username*> <*password*>

Syntax Description

<*hostname*>	Specifies the host name for the server that updates the dynamic domain naming system (DNS).
<*minutes*>	Specifies the intervals in minutes to update the server with information (updates also occur when the interface's IP address changes regardless of the update intervals).
<*username*>	Specifies a user name using an alphanumerical string up to 30 characters in length (the user name is case sensitive).
<*password*>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case sensitive). Refer to *Functional Notes* below for additional argument descriptions.

Default Values

No default values are necessary for this command.

Command History

Release 8.1	Command was introduced.
Release 12.1	Command was expanded.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release R10.10.0	Command was expanded to include the system management Ethernet virtual connection (EVC).

Functional Notes

custom - Constanttime.com's Custom Dynamic DNS^{SM} service allows you complete access and management control over your domain name regardless of where you purchased/registered it. This allows you to manage IP address mappings (A records), domain aliases (CNAME records), and mail servers (mail exchange (MX) records).

dyndns - The Dynamic DNS^{SM} offered by Dynamic Network Services, Inc. (DynDNS.org) allows you to alias a dynamic IP address to a static host name in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five host names.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for most common configurations and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to DynDNS.org's Dynamic DNS^{SM} service in that it allows a host name, such as yourname.dyndns.org, to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate through the DNS system. This service is provided for up to five host names.

If your IP address does not change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service that also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with host name **host**, user name **user**, and password **pass**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#dynamic-dns dyndns-custom host user pass**

ip access-group *<ipv4 acl name>*

Use the **ip access-group** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to be used for IPv4 packets transmitted on or received from the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable this type of control. Variations of this command include:

ip access-group <*ipv4 acl name*> **in**
ip access-group <*ipv4 acl name*> **out**

Syntax Description

<ipv4 acl name>	Applies the named IPv4 ACL to the EVC.
in	Enables access control on IPv4 packets received on the specified interface.
out	Enables access control on IPv4 packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

When this command is enabled, the IPv4 destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example configures the router to only allow IPv4 Telnet traffic (as defined in the user-configured **TelnetOnly** ACL) into the system management EVC:

(config)**#ip access-list extended TelnetOnly**
(config-ext-nacl)**#permit tcp any any eq telnet**
(config-ext-nacl)**#system-management-evc**
(config-sys-mgmt-evc)**#ip access-group TelnetOnly in**

ip access-policy *<ipv4 acp name>*

Use the **ip access-policy** command to assign a specified Internet Protocol version 4 (IPv4) access control policy (ACP) to the system management Ethernet virtual connection (EVC). IPv4 ACPs are applied to IPv4 traffic entering an interface. Use the **no** form of this command to remove an ACP association. For more information on using IPv4 ACPs, refer to *ip policy-class <ipv4 acp name> on page 1434*.

> NOTE *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv4 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<ipv4 acp name>	Identifies the configured IPv4 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv4 ACPs associated with an EVC.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 6.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*.

Usage Examples

The following example associates the IPv4 ACP **PRIVATE** (to allow inbound IPv4 traffic to the Web server) to the system management EVC:

Enable the AOS security features:
(config)**#ip firewall**

Associate the ACP with the system management EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip access-policy PRIVATE**

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

ip address dhcp class-id [ascii <*string*> **| hex** <*value*>**] [client-id [**<*interface*> **|** <*identifier*>**]] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp client-id [<*interface*> **|** <*identifier*>**] [hostname** <*"string"*>**] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp hostname *"*<*string*>*"* **[no-default-route | no-domain-name | no-nameservers] [track** <*name*>**] [**<*administrative distance*>**]**
ip address dhcp [no-default-route | no-domain-name | no-nameservers] [track <*name*>**] [**<*administrative distance*>**]**
ip address dhcp track <*name*> **[**<*administrative distance*>**]**

Syntax Description

<*administrative distance*>	Optional. Specifies the administrative distance to use when adding the DHCP gateway into the route table. It is used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more reliable the route. Range is **1** to **255**.
class-id	Optional. Specifies the vendor class identifier for the interface.
ascii <*string*>	Specifies the vendor class identifier in an ASCII string of up to **255** bytes.
hex <*value*>	Specfies the vendor class identifier in hexadecimal format. Valid range is up to **510** hexadecimal numbers. An even number of digits is required.
client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<*interface*>	Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address on page 4344* for a detailed listing of media types.
<*identifier*>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the <*identifier*> option.
hostname <*"string"*>	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field. The string is enclosed in quotation marks and can consist of up to 35 characters.

no-default-route Optional. Specifies that no default route is obtained via DHCP.

no-domain-name Optional. Specifies that no domain name is obtained via DHCP.

no-nameservers Optional. Specifies that no domain naming system (DNS) servers are obtained via DHCP.

track *<name>* Optional. Attaches a network monitoring track to the DHCP client. The DHCP gateway route for this client will only reside in the route table while the track is in the pass state. For more information on configuring track objects, refer to *track <name> on page 1886*.

Default Values

<administrative distance> By default, the administrative distance value is 1.

class-id Optional. By default, no vendor class identifier is configured.

client-id Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

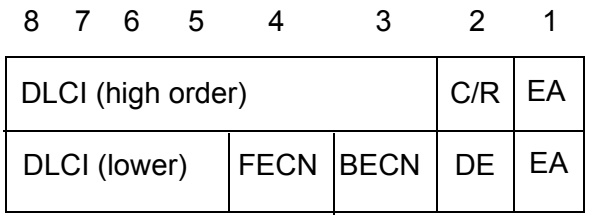
Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address on page 4344* for a detailed listing of media types), and the MAC ADDRESS is the medium access control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field.)

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:



Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname *“<string>”* By default, the host name is the name configured using the Global Configuration **hostname** command.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 13.1	Command was expanded to include the track and administrative distance.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.
Release R10.10.0	Command was expanded to include the **class-id** parameter in support of DHCP Option 60.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

The vendor class identifier is sent to the DHCP server in DHCP discover and request messages via DHCP Option 60. This option gives the DHCP server details regarding DHCP client configuration and also allows the server to send any vendor-specific information to the client in DHCP offer messages via Option 43.

Usage Examples

The following example enables DHCP operation on the interface:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip address dhcp**

The following example enables DHCP operation on the interface utilizing host name **adtran** and does not allow obtaining a default route, domain name, or name servers. It also sets the administrative distance as **5**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip address dhcp hostname “adtran” no-default-route no-domain-name no-nameservers 5**

ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the system management Ethernet virtual connection (EVC) (only one primary address is allowed). Use the optional **secondary** keyword to define a secondary IPv4 address. Use the **no** form of this command to remove a configured IPv4 address. Variations of this command include:

ip address <*ipv4 address*> <*subnet mask*>
ip address <*ipv4 address*> <*subnet mask*> **secondary**

Syntax Description

<*ipv4 address*>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
secondary	Optional. Configures a secondary IPv4 address for the EVC.

Default Values

By default, there are no assigned IPv4 addresses.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IPv4 address of **192.22.72.101 /30**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip address 192.22.72.101 /30 secondary**

ip address range *<start ipv4 address> <end ipv4 address> <subnet mask>* secondary

Use the **ip address range secondary** command to specify a range of secondary Internet Protocol version 4 (IPv4) addresses on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to remove the range of configured IPv4 addresses.

Syntax Description

<start ipv4 address>	Specifies the first IPv4 address in the range.
<end ipv4 address>	Specifies the last IPv4 address in the range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no IPv4 address range is defined.

Command History

Release 17.4	Command was introduced.
Release R10.1.0	Command was added to the facility data link (FDL) interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Use secondary IPv4 addresses to allow dual subnets on a single EVC (when you need more IPv4 addresses than the primary subnet can provide). When using secondary IPv4 addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IPv4 addresses on the secondary subnet.

Usage Examples

The following example configures a range of secondary IPv4 addresses from **192.22.72.1** to **192.22.72.10** on subnet **255.255.255.252**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip address range 192.22.72.1 192.22.72.10 255.255.255.252 secondary**

ip crypto map *<name>*

Use the **ip crypto map** command to associate Internet Protocol version 4 (IPv4) crypto maps with the system management Ethernet virtual connection (EVC). Use the **no** form of this command to remove a crypto map from an interface.

> NOTE *When you apply a map to an EVC, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name, but have different map index numbers.*

Syntax Description

<name>	Specifies the IPv4 crypto map name that you wish to assign to the EVC.

Default Values

By default, no crypto maps are assigned to an EVC.

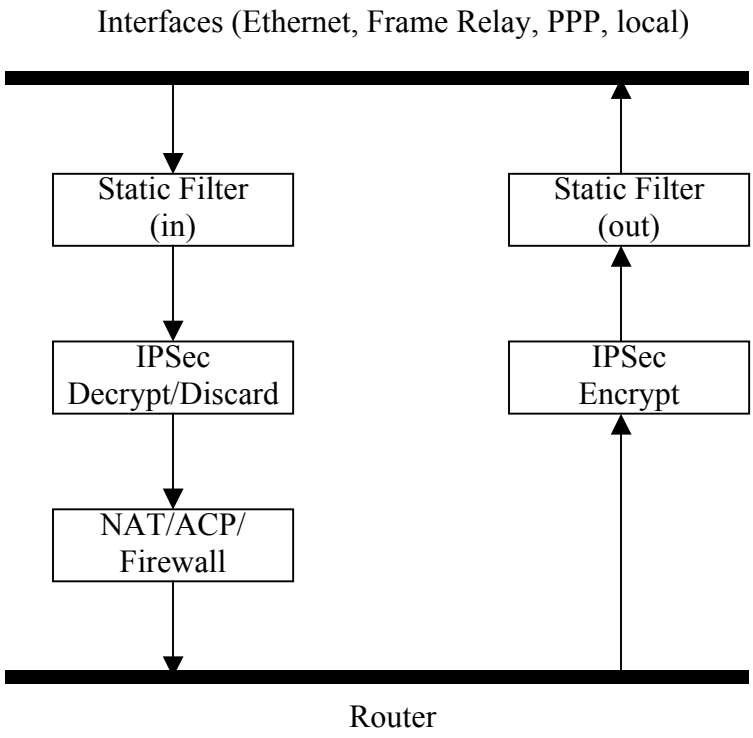
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release 8.1	Command was expanded to include the asynchronous transfer mode (ATM) subinterface.
Release 9.1	Command was expanded to include the High-Level Data Link Control (HDLC) interface.
Release 11.1	Command was expanded to include the demand interface.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

When configuring a system to use both the stateful inspection firewall and Internet key exchange (IKE) negotiation for VPN, keep the following notes in mind.

When defining the IPv4 policy class and associated access control lists (ACLs) that describe the behavior of the IPv4 firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the EVC on which the data is received. This access group is a true static filter and is available for use regardless of whether the IPv4 firewall is enabled or disabled. Next (if the data is encrypted), it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The IPv4 ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an EVC. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far-end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all IPv4 crypto maps with the name **MyMap** to the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip crypto map MyMap**

ip dhcp

Use the **ip dhcp** command to release or renew the Dynamic Host Configuration Protocol (DHCP) Internet Protocol version 4 (IPv4) address. This command is only applicable when using DHCP for IP address assignment. Variations of this command include:

ip dhcp release
ip dhcp renew

Syntax Description

release	Releases the DHCP IPv4 address.
renew	Renews the DHCP IPv4 address.

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.
Release 8.1	Command was added to the asynchronous transfer mode (ATM) subinterface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R10.1.0	Command was added to the bridged virtual interface (BVI).
Release R10.10.0	Command was expanded to include the system management Ethernet virtual connection (EVC).

Usage Examples

The following example releases the IPv4 address assigned (by DHCP) on the system management EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip dhcp release**

ip dhcp relay destination *<ipv4 address>*

Use the **ip dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 4 (IPv4) and to specify the IPv4 address for the DHCPv4 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv4 relay functionality is disabled on the interface.

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the DHCPv4 messages. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**)..

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.10.0	Command was expanded to include the system management Ethernet virtual connection (EVC).

Usage Examples

The following example enables DHCPv4 relay agent functionality and specifies the destination address as **192.33.4.251**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip dhcp relay destination 192.33.4.251**

ip directed-broadcast

Use the **ip directed-broadcast** command to allow reception/forwarding of directed broadcasts. Use the **no** form of this command to disable this feature. Variations of this command include:

ip directed-broadcast
ip directed-broadcast <*name*>

Syntax Description

<*name*>	Specifies IP access control list (ACL) name.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management Ethernet virtual connection (EVC).

Functional Notes

A directed broadcast is a packet intended for all nodes on a nonlocal network. For example, the broadcast address 255.255.255.255 reaches all nodes on a network; the directed broadcast address 128.1.255.255 is intended for all nodes whose network address is 128.1.0.0. A router not directly attached to 128.1.0.0 simply forwards the directed broadcast packet to the next hop. A router on network 128.1.0.0 that has **ip directed-broadcast** enabled, accepts and forwards the packet to all nodes whose network address is 128.1.0.0. Routers connecting subnets of 128.1.0.0 also accept and forward the packet to the nodes on their respective subnets. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is distributed as a broadcast on the destination subnet. The packet is then sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the distribution of directed broadcasts when they reach their target subnets. Only the final transmission of the directed broadcast on its ultimate destination subnet is affected. It does not affect the transit unicast routing of IP directed broadcasts.

If **ip directed-broadcast** is enabled for this interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which this EVC is attached will be forwarded as broadcasts on that subnet. Forwarding of the packets can be limited by specifying an ACL with this command. In this case, only directed broadcasts that are permitted by the specified ACL will be forwarded, and all other directed broadcasts directed to this EVC subnet will be dropped.

Disabling the **ip directed-broadcast** command will cause directed broadcasts destined for the subnet to which this EVC is attached to be dropped.

This option is a requirement for routers as described in RFC 1812, section 4.2.2.11. Furthermore, it is disabled by default (RFC 2644), with the intended goal of reducing the efficacy of certain types of denial of service (DoS) attacks.

Usage Examples

The following example enables forwarding of directed broadcasts on the system management EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip directed-broadcast**

ip flow

Use the **ip flow** command to enable integrated traffic monitoring (ITM) for all traffic received or forwarded on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable traffic monitoring. Variations of this command include:

ip flow egress
ip flow egress <*name*>
ip flow ingress
ip flow ingress <*name*>

Syntax Description

egress	Specifies that all outgoing traffic be monitored.
ingress	Specifies that all incoming traffic be monitored.
<*name*>	Optional. Specifies the name of an access control list (ACL) to use for filtering traffic.

Default Values

By default, no traffic monitoring is enabled.

Command History

Release 16.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Usage Examples

The following example enables traffic monitoring on the system management EVC to monitor **incoming** traffic through an ACL called **MYACL**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip flow ingress MYACL**

ip helper-address *<ipv4 address>*

Use the **ip helper-address** command to configure AOS to forward User Datagram Protocol (UDP) broadcast packets received on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <value> on page 1398 for more information.*

Syntax Description

<ipv4 address>	Specifies the destination IP address for the forwarded UDP packets. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, broadcast UDP packets are not forwarded.

Command History

Release 1.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is UDP.
2. Any UDP port specified using the **ip forward-protocol** command.
3. The medium access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IPv4 address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248 /30 subnet).

Usage Examples

The following example forwards all domain naming system (DNS) broadcast traffic to the DNS server with IPv4 address **192.33.5.99**:

(config)**#ip forward-protocol udp domain**
(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip helper-address 192.33.5.99**

ip mtu <*size*>

Use the **ip mtu** command to configure the Internet Protocol version 4 (IPv4) maximum transmission unit (MTU) size for the system management Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Configures the window size for transmitted IPv4 packets. The valid ranges for the various interfaces are listed below:	
	ATM subinterfaces	64 to 1520
	BVIs	64 to 2100
	Demand interfaces	64 to 1520
	Ethernet interfaces (all types)	64 to 1500
	FDL interfaces	64 to 256
	Frame Relay subinterfaces	64 to 1520
	HDLC interfaces (NetVanta 5305)	64 to 4600
	HDLC interfaces (all other NetVanta products)	64 to 2100
	Loopback interfaces	64 to 1500
	PPP interfaces (NetVanta 5305)	64 to 4600
	PPP interfaces (all other NetVanta products)	64 to 2100
	Tunnel interfaces	64 to 18190

Default Values

<*size*>	The default values for the various interfaces are listed below:	
	ATM subinterfaces	1500
	BVIs	1500
	Demand interfaces	1500
	Ethernet interfaces (all types)	1500
	FDL interfaces	256
	Frame Relay subinterfaces	1500
	HDLC interfaces	1500
	Loopback interfaces	1500
	PPP interfaces	1500
	Tunnel interfaces	1476

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.
Release 17.9	Command was changed to require the **ip** keyword for Adtran internetworking products only.
Release R10.1.0	Command was changed to require the **ip** keyword for Adtran voice products.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

OSPFv2 will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an IPv4 MTU of 1200 on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip mtu 1200**

ip policy route-map *<name>*

Use the **ip policy route-map** command to assign a policy route-map to the system management Ethernet virtual connection (EVC). Use the **no** form of this command to remove the route-map policy.

Syntax Description

<name>	Specifies the name of the policy route map to assign to this EVC.

Default Values

By default, no policy route map is assigned to this EVC.

Command History

Release 11.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Usage Examples

The following example assigns the policy route map **policy1** to the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip policy route-map policy1**

ip proxy-arp

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, proxy ARP is enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, AOS will respond to all ARP requests with its specified medium access control (MAC) address and forward packets accordingly.

Enabling proxy ARP on an EVC may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip proxy-arp**

ip rip authentication

Use the **ip rip authentication** command to enable specify the Internet Protocol version 4 (IPv4) Routing Information Protocol (RIP) authentication method on the Ethernet virtual connection (EVC). Use the **no** form of this command to disable RIP authentication. Variations of this command include:

ip rip authentication key-chain <*name*>
ip rip authentication mode md5
ip rip authentication mode text

Syntax Description

key-chain <*name*>	Specifies that RIP authentication is completed using an authentication key, and specifies the key name.
mode md5	Specifies that RIP authentication is completed using message digest authentication.
mode text	Specifies that RIP authentication is completed using clear text authentication.

Default Values

By default, RIP authentication is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables RIP authentication on the EVC and specifies authentication is completed using clear text:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#**

ip rip receive version

Use the **ip rip receive version** command to configure the Routing Information Protocol (RIP) version the unit accepts in all RIP packets received on the system management Ethernet virtual connection (EVC). Variations of this command include:

ip rip receive version 1
ip rip receive version 2

Syntax Description

1	Accepts only RIP version 1 packets received on the EVC.
2	Accepts only RIP version 2 packets received on the EVC.

Default Values

By default, the EVC implements RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only accepts one version (either **1** or **2**) on an EVC.

Usage Examples

The following example configures the EVC to accept only RIP version **2** packets:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip rip receive version 2**

ip rip send version

Use the **ip rip send version** command to configure the Routing Information Protocol (RIP) version the unit sends in all RIP packets transmitted on the system management Ethernet virtual connection (EVC). Variations of this command include:

ip rip send version 1
ip rip send version 2

Syntax Description

1	Transmits only RIP version 1 packets on the EVC.
2	Transmits only RIP version 2 packets on the EVC.

Default Values

By default, the EVC transmit RIP version **1** (the default value for the **version** command).

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version on page 4220* for more information.

AOS only transmits one version (either **1** or **2**) on an EVC.

Usage Examples

The following example configures the EVC to transmit only RIP version **2** packets:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip rip send version 2**

ip rip summary-address *<ipv4 address> <subnet mask>*

Use the **ip rip summary-address** command to manually summarize the routes Routing Information Protocol (RIP) will advertise and send out the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable this mode.

Syntax Description

<ipv4 address>	Specifies the summarized network IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.0**).
<subnet mask>	Specifies the subnet mask that corresponds to the range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, no manual summarization is applied by RIP.

Command History

Release 12.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Unlike the automatic summarization on classful network boundaries, only specific network advertisements are made by RIP using the **ip rip summary-address** command. This command is only effective if RIP version 2 is configured.

Usage Examples

The following example enables manual summarization on the specified IPv4 address:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip rip summary-address 10.10.123.0 255.255.255.0**

ip route-cache

Use the **ip route-cache** command to enable Internet Protocol version 4 (IPv4) fast-cache switching on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

*Using network address translation (NAT) or the AOS firewall capabilities on an EVC requires process switching mode (using the **no ip route-cache** command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on the EVC.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Fast switching allows an EVC to provide optimum performance when processing IPv4 traffic.

Usage Examples

The following example enables IPv4 fast switching on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip route-cache**

ip split-horizon

Use the **ip split-horizon** command to enable Internet Protocol version 4 (IPv4) Routing Information Protocol (RIP) split horizon on the Ethernet virtual connection (EVC). Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, RIP split horizon is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables RIP split horizon on the EVC:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#ip split-horizon
```

ip urlfilter *<name>*

Use the **ip urlfilter** command to apply a universal resource locator (URL) filter to the system management Ethernet virtual connection (EVC) for all inbound or outbound traffic. Use the **no** form of this command to remove the URL filter from the EVC. Variations of this command include:

ip urlfilter <*name*> **in**
ip urlfilter <*name*> **out**

Syntax Description

<name>	Specifies the URL filter name to use on the EVC.
in	Applies the filter to the inbound traffic.
out	Applies the filter to the outbound traffic.

Default Values

By default, there are no URL filters applied to any EVCs.

Command History

Release 12.1	Command was introduced.
Release 14.1	Command was expanded to include the virtual local area network (VLAN) interfaces.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

The firewall must be enabled using the **ip firewall** command in order to use URL filters. The URL filter must be created by using the **ip urlfilter** *<filter name>* **http** command before applying it to the EVC. Refer to *ip urlfilter <name> http on page 1495* for more information on using this command.

Usage Examples

The following example performs URL filtering on all traffic entering through the EVC and matches the URL filter named **MyFilter**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ip urlfilter MyFilter in**

ipv6

Use the **ipv6** command to enable Internet Protocol version 6 (IPv6) processing and create a link-local address on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable IPv6 processing and remove all IPv6 configuration on the EVC.

Syntax Description

No subcommands.

Default Values

By default, IPv6 is not enabled on the EVC.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Because AOS uses the dual-stack for IPv6 implementation, IPv6 features must be enabled for the supported IPv6 features to be used. Enabling IPv6 in AOS is completed by using an IPv6 address or using the **ipv6** keyword with specific commands. For example, to enable IPv6 on an interface and cause the EVC to join the link scoped all-nodes and all-routers multicast group, enter an IPv6 address on the EVC.

Use the **ipv6** command to enable IPv6 processing and create a link-local address on an EVC when other unicast IPv6 addresses are not needed on the EVC. This command is not necessary nor effectual when any other form of an IPv6 address command is also present on the EVC.

Usage Examples

The following example enables IPv6 and creates a link-local IPv6 address on the EVC:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#ipv6
```


ipv6 access-group *<ipv6 acl name>*

Use the **ipv6 access-group** command to apply an Internet Protocol version 6 (IPv6) access control list (ACL) to be used for IPv6 packets transmitted on or received from the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable this type of control. Variations of this command include:

ipv6 access-group *<ipv6 acl name>* **in**
ipv6 access-group *<ipv6 acl name>* **out**

Syntax Description

<ipv6 acl name>	Applies the named IPv6 ACL to the EVC.
in	Enables access control on IPv6 packets received on the EVC.
out	Enables access control on IPv6 packets transmitted on the EVC.

Default Values

By default, these commands are disabled.

Command History

Release 18.1	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Only one IPv6 ACL can be applied in each traffic direction.

Unlike in IPv4, IPv6 traffic filters include an implicit **permit** for neighbor solicitation and advertisement packets in an ACL before the traditional implicit **deny** at the end of the ACL. This prevents blocking of address resolution and unreachability detection, although this can be overridden by entering explicit **deny** commands in the IPv6 ACL.

Usage Examples

The following example applies the IPv6 ACL **Privatev6** to incoming IPv6 traffic on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 access-group Privatev6 in**

ipv6 access-policy *<ipv6 acp>*

Use the **ipv6 access-policy** command to assign a specified Internet Protocol version 6 (IPv6) access control policy (ACP) to the system management Ethernet virtual connection (EVC). IPv6 ACPs are applied to IPv6 traffic entering the EVC. Use the **no** form of this command to remove an ACP association.

Syntax Description

<ipv6 acp>	Identifies the configured IPv6 ACP by alphanumeric descriptor (all ACP descriptors are case sensitive).

Default Values

By default, there are no configured IPv6 ACPs associated with the EVC.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Usage Examples

The following example applies the IPv6 ACP **PRIVATEv6** to the EVC:

Enable the AOS security features:
(config)**#ipv6 firewall**

Associate the ACP with the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 access-policy PRIVATEv6**

ipv6 address autoconfig

Use the **ipv6 address autoconfig** command to enable Internet Protocol version 6 (IPv6) processing on the system management Ethernet virtual connection (EVC), create a local-link IPv6 address for the EVC, and allow the EVC to automatically configure itself based on advertisements from other routers on the link. Use the **no** form of this command to remove all autoconfigured addresses, prefixes, and any resulting routes from the EVC and also causes the EVC to cease processing received router advertisements (RAs).Variations of this command include:

ipv6 address autoconfig
ipv6 address autoconfig default
ipv6 address autoconfig default metric <*value*>

Syntax Description

default	Optional. Specifies that the EVC maintain a list of advertising routers that are willing to be IPv6 default routers.
metric <*value*>	Optional. Specifies the administrative distance for a default router maintained in the default router list. Range is **1** to **255**. Routes with lower administrative distance are favored.

Default Values

By default, no IPv6 addresses are configured for the EVC and IPv6 processing is not enabled. When an IPv6 address is configured automatically, the administrative distance for default routers is **2** by default.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

When autoconfiguration is enabled, the EVC listens for RA messages that tell the EVC how it should be configured. The EVC then creates addresses for advertised 64-bit prefixes with the A flag in the IPv6 address set using stateless address autoconfiguration (SLAAC). The addresses use the EUI-64 interface ID in the lower 64 bits of the address. A route type of *Connected* is added to the route table if the L flag on the prefix advertisement (on-link flag) is also set.

Usage Examples

The following example enables IPv6 processing on the EVC, creates a link-local IPv6 address for the EVC, and allows the EVC to automatically configure itself for IPv6:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 address autoconfig**

ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to remove the IPv6 address from the EVC.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, no IPv6 address is configured on the EVC and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the EVC using the command *ipv6 address <ipv6 link-local address> link-local on page 3882*.

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the EVC. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the EVC.

Usage Examples

The following example adds a unicast IPv6 address to the EVC and enables IPv6 processing on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 address 2001:DB8::/32**

ipv6 address *<ipv6 prefix/prefix-length>* eui-64

Use the **ipv6 address eui-64** command to assign a unicast Internet Protocol version 6 (IPv6) address and enable IPv6 processing on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to remove the IPv6 address from the EVC.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
eui-64	Specifies that the IPv6 address is constructed using the specified prefix in the high-order bits and followed by the EUI-64 Interface ID in the lower 64 bits.

Default Values

By default, no IPv6 address is configured on the EVC and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**). Link-local addresses are created on the EVC using the command *ipv6 address <ipv6 link-local address> link-local on page 3882*.

The address created by this command is an EUI-64 unicast address. For this type of address, the EUI-64 interface ID is automatically placed in the IPv6 address. Any manually configured bits beyond the address's prefix length are set to **0**; however, any manually configured bits within the prefix length that extend into the lower 64 bits take precedence over the Interface ID bits.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the EVC. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the EVC.

Usage Examples

The following example adds a unicast IPv6 address with an EUI-64 Interface ID to the EVC and enables IPv6 processing on the EVC:

(config)#**system-management-evc**
(config-sys-mgmt-evc)#**ipv6 address 2001:DB8:3F::/48 eui-64**

ipv6 address <*ipv6 link-local address*> link-local

Use the **ipv6 address link-local** command to manually assign a link-local Internet Protocol version 6 (IPv6) address to the system management Ethernet virtual connection (EVC) and enable IPv6 processing on the EVC. Use the **no** form of this command to remove the IPv6 address from the EVC.

Syntax Description

<*ipv6 link-local address*>	Specifies the link-local IPv6 address. Link-local addresses are specified in colon hexadecimal notation, and begin with **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
link-local	Specifies this is a manually configured link-local address. Manually configured link-local addresses replace automatically configured link-local addresses on the EVC.

Default Values

By default, no IPv6 address is configured for the EVC and IPv6 processing is not enabled.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

A single link-local address can be manually configured on an EVC. The lower 64 bits of the specified address become the Interface ID for the EVC, overriding the default interface ID. Any other address that uses the EUI-64 parameter to automatically place the interface ID in the lower 64 bits of the IPv6 address use the new value for the interface ID.

The <*ipv6 address*> for a link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since this form of address has no prefix, the bits entered form the entire IPv6 address. These bits also become the new interface ID for the EVC and can be derived from the EVC's medium access control (MAC) address.

The **link-local** parameter specifies this is a manually configured link-local address. Any manually configured link-local address will replace an automatically configured link-local address for the EVC.

Using the **no** form of this command with a specified IPv6 address removes that IPv6 address from the EVC. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the EVC.

Usage Examples

The following example manually creates a link-local IPv6 address on the EVC and enables IPv6 processing:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 address FE80::220:8FF:FE54:F9D8 link-local**

ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

ipv6 address dhcp
ipv6 address dhcp hostname <*partial fqdn*>
ipv6 address dhcp hostname fqdn <*fqdn*>
ipv6 address dhcp no-domain-name
ipv6 address dhcp no-nameservers
ipv6 address dhcp no-ntp
ipv6 address dhcp no-sntp-server
ipv6 address dhcp rapid-commit

Syntax Description

hostname <*partial fqdn*>	Optional. Specifies the name to be sent to the DHCPv6 server as the host portion of its fully qualified domain name (FQDN). FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
fqdn <*fqdn*>	Optional. Specifies a name to be sent to the DHCPv6 server as the system's FQDN. FQDNs are expressed in ASCII text of up to **254** characters. The string can be enclosed in quotation marks.
no-domain-name	Optional. Specifies that no domain names are obtained using this DHCPv6 client.
no-nameservers	Optional. Specifies that no domain naming server (DNS) addresses are obtained through DHCPv6.
no-ntp	Optional. Specifies that no Network Time Protocol (NTP) server values are obtained through this DHCPv6 client.
no-sntp-server	Optional. Specifies that no Simple Network Time Protocol (SNTP) server values are obtained through this DHCPv6 client.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Functional Notes

To enable an interface as a DHCPv6 client, you must first enable IPv6 on the interface using the command *ipv6 on page 3876*.

Enabling the interface as a DHCPv6 client using the **ipv6 address dhcp** command places the interface into DHCPv6 client mode. DHCPv6 modes (**client**, **server**, **relay**) are mutually exclusive at the interface. Any existing mode must be removed before a different mode can be applied. For example, if the interface is configured as a DHCPv6 relay agent, you must first disable the **relay** mode before you can specify the interface is in **client** mode.

Usage Examples

The following example enables the interface as a DHCPv6 client and specifies the client's host name:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 address 2001:DB8:1::1/64**
(config-sys-mgmt-evc)**#ipv6 address dhcp fqdn client@company.com**

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*

Use the **ipv6 address named-prefix** command to create an Internet Protocol version 6 (IPv6) address for the Ethernet virtual connection (EVC) using the values in a named prefix. Use the **no** form of this command to remove the address from the EVC. Variations of this command include:

ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>*
ipv6 address named-prefix *<prefix name> <ipv6 address/prefix-length>* **eui-64**

Syntax Description

<prefix name>	Specifies the named prefix to use to create the address.
<ipv6 address/prefix-length>	Specifies the address portion appended to the named prefix to create a 128-bit host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
eui-64	Optional. Indicates that the interface ID is to be placed in the lower 64 bits of the address.

Default Values

By default, no IPv6 addresses are specified on the EVC.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.

Usage Examples

The following example creates an IPv6 address on the EVC using the named prefix **PREFIX1**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 address named-prefix PREFIX1 2001:1:0:/48**

ipv6 crypto map *<name>*

Use the **ipv6 crypto map** command to associate Internet Protocol version 6 (IPv6) crypto maps with the system management Ethernet virtual connection (EVC). Use the **no** form of this command to remove a crypto map from the EVC.

Syntax Description

<name>	Specifies the IPv6 crypto map name that you wish to assign to the EVC.

Default Values

By default, no crypto maps are assigned to an EVC.

Command History

Release R10.7.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Only one IPv6 crypto map can be specified per EVC, and the crypto map is applied within the virtual routing and forwarding (VRF) instance to which the EVC belongs. To apply the IPv6 crypto map, the EVC must have IPv6 enabled. In addition, the EVC must have an IPv6 address of appropriate scope to allow connectivity to peer's addresses as specified in the crypto map's entries.

Usage Examples

The following example applies all IPv6 crypto maps with the name **MyMap** to the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6**
(config-sys-mgmt-evc)**#ipv6 crypto map MyMap**

ipv6 dhcp client information refresh minimum <*seconds*>

Use the **ipv6 dhcp client information refresh minimum** command to specify the minimum value the Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) client on the system management Ethernet virtual connection (EVC) accepts as its information refresh timer. Use the **no** version of this command to return to the default setting.

Syntax Description

<*seconds*>	Specifies the refresh timer in seconds. Valid range is **600** to **3600** seconds.

Default Values

By default, the DHCPv6 client refresh timer is set to **600** seconds.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Usage Examples

The following example specifies the DHCPv6 client refresh timer for the EVC is **800** seconds:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 dhcp client information refresh minimum 600**

ipv6 dhcp client pd <*prefix name*>

Use the **ipv6 dhcp client pd** command to enable the Dynamic Control Host Protocol for Internet Protocol version 6 (DHCPv6) client on the interface and specify that the interface acquires an IPv6 prefix for the DHCPv6 client. Use the **no** form of this command to disable this feature. Variations of this command include:

ipv6 dhcp client pd <*prefix name*>
ipv6 dhcp client pd <*prefix name*> **no-aggregate-route**
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*>
ipv6 dhcp client pd <*prefix name*> **distance** <*distance*> **tag** <*value*>
ipv6 dhcp client pd <*prefix name*> **rapid-commit**

Syntax Description

<*prefix name*>	Specifies the variable of the prefix stored on the AOS system. Variables are expressed in ASCII text of up to **80** characters.
no-aggregate-route	Optional. Specifies that a route to the null 0 interface is not injected into the route table for the prefixes assigned.
distance <*distance*>	Optional. Specifies the administrative distance to assign to the injected route. Valid range is **1** to **255** with a default distance of **1**.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.
tag <*value*>	Optional. Specifies a number to use as a tag for labeling and filtering routers. Valid range is **1** to **65535**.

Default Values

By default, the DHCPv6 client mode is not enabled on the interface.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.
Release R11.1.0	Command was expanded to include the **rapid-commit** parameter.

Usage Examples

The following example enables the DHCPv6 client on the interface and assigns the prefix **PREFIX1**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 dhcp client pd PREFIX1**

ipv6 dhcp relay destination *<ipv6 address>*

Use the **ipv6 dhcp relay destination** command to enable Dynamic Host Control Protocol (DHCP) for Internet Protocol version 6 (IPv6) and to specify the IPv6 address for the DHCPv6 messages. Using the **no** form of this command disables the relay functionality for the specified destination. When all destinations are removed, DHCPv6 relay functionality is disabled on the system management Ethernet virtual connection (EVC). Variations of this command include:

ipv6 dhcp relay destination *<ipv6 address>*
ipv6 dhcp relay destination *<ipv6 address>* *<interface>*
ipv6 dhcp relay destination *<ipv6 address>* **system-control-evc**
ipv6 dhcp relay destination *<ipv6 address>* **system-management-evc**

Syntax Description

<ipv6 address>	Specifies the IPv6 address for the DHCPv6 messages. IPv6 addresses should be specified in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<interface>	Optional. Specifies an output interface to use when sending messages to the DHCPv6 server. If no interface is specified, the interface is selected by the routing table. This parameter is only required when the IPv6 address is a link-scoped address. Interfaces are specified in the *<interface type> <slot/port | interface id>* format. For example, for an Ethernet interface, use **eth 0/1**. Type **ipv6 dhcp relay destination** *<ipv6 address>* **?** to display a list of valid interfaces.
system-control-evc	Optional. Specifies the output interface for sending messages to the DHCPv6 server is the system control EVC.
system-management-evc	Optional. Specifies the output interface for sending messages to the DHCPv6 server is the system management EVC.

Default Values

By default, no DHCP relay agent destinations are configured and the relay agent mode is disabled.

Command History

Release 18.2	Command was introduced.
Release R10.1.0	Command was expanded to include the tunnel interface.
Release R10.5.0	Command was expanded to include the loopback interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

To configure an EVC to function as a DHCPv6 relay agent, you must first enable IPv6 on the EVC using the command *ipv6 on page 3876*.

Usage Examples

The following example enables DHCPv6 relay agent functionality and specifies the destination address as **2001:DB8:2::1**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6**
(config-sys-mgmt-evc)**#ipv6 dhcp relay destination 2001:DB8:2::1**

Technology Review

DHCPv6, like DHCP in IPv4, is used in IP networks to supply hosts with IP addresses and other networking information. DHCPv6, however, functions slightly differently than DHCPv4 by providing relay agents with the ability to send relay-forward and relay-reply messages. In addition, in DHCPv4, when DHCP messages are sent to a DHCP server whose address is not known, the IPv4 client uses the broadcast address. In DHCPv6, the IPv6 client sends messages using the link-scoped mulitcast address. This address is the All DHCP Relay Agents and Servers link, designated as **FF02::1:2**.

In AOS, DHCPv6 relay agents are used when the DHCP server is not on the same link as the DHCP client. The relay is typically a router on the same link as the client, which acts as an intermediary to help the client's DHCP messages reach the DHCP server. DHCPv6 relay agents operate transparently to the DHCP client, and can be configured in chains, meaning that information about each agent encountered is encapsulated into the relay message. Relay agents add fields to the DHCP message as they send these messages to the server, thus providing a method to properly manage the DHCP client.

For more information about DHCPv6 functionality in AOS, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

ipv6 dhcp server

Use the **ipv6 dhcp server** command to enable Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) on the system management Ethernet virtual connection (EVC) and specify that the EVC is functioning as a DHCPv6 server. This command not only enables the DHCPv6 server on the EVC, it also configures specific parameters of the DHCPv6 server. Hence, the parameters of this command can be entered multiple times and in any order. Use the **no** form of this command to disable DHCPv6 on the EVC. Variations of this command include:

ipv6 dhcp server automatic
ipv6 dhcp server automatic allow-hint
ipv6 dhcp server automatic preference <*number*>
ipv6 dhcp server automatic rapid-commit
ipv6 dhcp server <*pool name*>
ipv6 dhcp server <*pool name*> **allow-hint**
ipv6 dhcp server <*pool name*> **preference** <*number*>
ipv6 dhcp server <*pool name*> **rapid-commit**

Syntax Description

automatic	Enables automatic selection of the DHCPv6 server pool based on information extracted from the DHCPv6 client's request. You must specify the pool selection method before configuring other options for this command.
<*pool name*>	Specifies the DHCPv6 server pool that services this EVC. All DHCPV^ requests received on this EVC are serviced from this pool. If a pool name is not specified, the server pool is selected automatically. You must specify the pool selection method before configuring the other options for this command.
allow-hint	Optional. Specifies that the DHCPv6 server attempts to honor the DHCPv6 client's request for specific values as hinted in the client's request (if they are valid and not already assigned). If this option is not specified, any hints from the DHCPv6 client are ignored.
preference <*number*>	Optional. Specifies the preference value advertised by the server. This option is sent by the server to a DHCPv6 client to influence the selection of a server when there are multiple servers from which to choose. Valid range is **0** to **255**, with a default value of **0**. When the preference value is set to a non-zero value, the server includes a preference option containing the value. If the preference value is not set, or is set to 0, the option is omitted and the client assumes the value is 0.
rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

Default Values

By default, DHCPv6 server mode is not enabled on the EVC.

Command History

Release R10.1.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Enabling the EVC as a DHCPv6 server using this command places the EVC into DHCPv6 server mode. DHCPv6 modes (server, client, or relay) are mutually exclusive at the EVC. Any existing mode will be removed if a different mode is specified, and a message will be shown indicating the change in DHCPv6 mode.

Usage Examples

The following example enables the EVC as a DHCPv6 server, and specifies that the DHCPv6 server pool **POOL1** is associated with the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 address 2001:DB8:1::1/64**
(config-sys-mgmt-evc)**#ipv6 dhcp server POOL1**

ipv6 mode host unicast

Use the **ipv6 mode host unicast** command to place the system management Ethernet virtual connection (EVC) in host mode using an Internet Protocol version 6 (IPv6) unicast address. Use the **no** form of this command to disable host mode on the EVC.

Syntax Description

No subcommands.

Default Values

By default, host mode is disabled.

Command History

Release R10.9.0	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Command History

When this command is configured on an interface, the MTU value is learned from received router advertisements. Link MTU value is learned in host mode from the following locations (in decreasing order of priority): the provisioned MTU value in the interface configuration, the router advertisements received on the interface, and the default MTU value (1500).

Usage Examples

The following example places the EVC in host mode:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 mode host unicast**

ipv6 mtu *<size>*

Use the **ipv6 mtu** command to specify the maximum transmission unit (MTU) for Internet Protocol version 6 (IPv6) packets on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Specifies the MTU value. Valid range is **1280** to **1500** bytes.

Default Values

By default, the MTU of the EVC is set to **1280** bytes.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

In IPv6, the minimum MTU is 1280 octets. Any link that has an MTU less than 1280 octets must use link fragmentation and reassembly that is transparent to IPv6 (for example, the Fragmentation Header). Sources in the IPv6 network are expected to perform path maximum transmission unit (PMTU) discovery to send packets larger than 1280 octets. PMTU works in the following manner: First, the sending node assumes the link MTU of the interface from which the traffic is being forwarded and then sends the IPv6 packet at the link MTU size. If a router on the path is unable to forward the packet, it sends an ICMP *Packet Too Big* message back to the sending node containing the link MTU of the link on which the packet forwarding failed. The sending node then rests the PMTU to the value of the MTU field in the Internet Control Message Protocol version 6 (ICMPv6) *Packet Too Big* message, and the packet is resent.

The MTU for IPv6 packets can be set on a per-EVC basis. There are two methods for setting MTUs for EVCs if required: one for Layer 3 EVCs, and one for the underlying Layer 1 and Layer 2 EVCs. For all EVC types, use the **ipv6 mtu** *<size>* command to specify the IPv6 MTU in bytes from the EVC's configuration mode. The minimum MTU setting for IPv6 is **1280** bytes, and the maximum is **1500** bytes. The IPv6 MTU value is independent of the IPv4 MTU setting (set with the command *ip mtu <size> on page 3865*).

When the EVC is forwarding the IPv6 packet as a router, if the packet size exceeds the IPv6 MTU of the egress EVC, the packet is dropped and ICMPv6 *Packet Too Big* message is sent to the source. When originating an IPv6 packet from the local IPv6 stack, and the packet is larger than the IPv6 MTU of the egress EVC, the packet is fragmented and sent.

Usage Examples

The following example specifies the IPv6 MTU value for the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 mtu 1350**

ipv6 nd advertisement-interval

Use the **ipv6 nd advertisement-interval** command to specify that the Advertisement Interval Option is sent in Internet Protocol version 6 (IPv6) router advertisement (RA) messages from the router. This command is effectual only when the system management Ethernet virtual connection (EVC) is in router mode. Use the **no** form of this command to return to the default interval.

Syntax Description

No subcommands.

Default Values

By default, Advertisement Interval Options are not sent in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Sending the Advertisement Interval Option should be enabled when the router is functioning in a mobile IP environment to aid movement detection by mobile nodes. This option contains the current value of the maximum router advertisement interval configured using the command *ipv6 nd ra interval on page 3906*.

Usage Examples

The following example specifies that the EVC include Advertisement Interval Options in RA messages sent from the router:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd advertisement-interval**

ipv6 nd cache max-incomplete <*number*>

Use the **ipv6 nd cache max-incomplete** command to specify the maximum number of incomplete entries the Neighbor Discovery (ND) cache retains. Use the **no** form of this command to return to the default value.

Syntax Description

<*number*>	Specifies the number of incomplete ND entries to retain in the cache. Valid range is **1** to **321**.

Default Values

By default, the incomplete ND entries can take at maximum one-third of the possible ND cache entries (varies by product).

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example specifies that the interface stores **150** incomplete entries in the ND cache:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd cache max-incomplete 150**

ipv6 nd dad attempts *<number>*

Use the **ipv6 nd dad attempts** command to specify the number of neighbor solicitation (NS) messages sent by the system management Ethernet virtual connection (EVC) when performing Internet Protocol version 6 (IPv6) duplicate address detection (DAD). This command is effectual when the EVC is in either host or router mode. Use the **no** form of this command to return to the default value.

Syntax Description

<number>	Specifies the number of NS messages that will be sent. Range is **0** to **10** messages. A value of **0** disables DAD on the interface.

Default Values

By default, the EVC sends **1** NS message.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

DAD is used by devices to determine if IPv6 addresses are unique before they are applied to EVCs. DAD is used in NS messages to detect duplicate unicast addresses. The Target Address fields in the NS messages are set to the IPv6 address for which duplication is being detected. Destination IPv6 addresses for DAD in NS messages are the solicited-node multicast version of the address being tested. Source IPv6 addresses for DAD are set to the IPv6 unspecified address (::). Once the IPv6 address is determined by DAD to be unique, it can be applied to the EVC on the node.

DAD in AOS is performed when an EVC transitions state from DOWN to UP or when manually configuring an address. When performing DAD because of an interface transition, DAD will happen immediately after the EVC transition and again 40 seconds later to cooperate with the port being connected to an Ethernet switch.

Usage Examples

The following example specifies that **3** NS messages are sent by the EVC when performing DAD:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd dad attempts 3**

ipv6 nd generate-packet

Use the **ipv6 nd generate-packet** command to generate and send test packets from the Ethernet virtual connection (EVC) for Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages. Use the **no** form of this command to disable packet generation. Variations of this command include:

ipv6 nd generate-packet neighbor-advertisement <*source ipv6 address*> <*destination ipv6 address*> <*Layer 2 address*>
ipv6 nd generate-packet neighbor-solicitation <*source ipv6 address*> <*destination ipv6 address*> <*target ipv6 address*>
ipv6 nd generate-packet router-advertisement

Syntax Description

neighbor-advertisement	Specifies that test packets are generated for neighbor advertisement (NA) messages.
neighbor-solicitation	Specifies that test packets are generated for neighbor solicitation (NS) messages.
router-advertisement	Specifies that test packets are generated for router advertisement (RA) messages.
<*source ipv6 address*>	Specifies the source address of the test packet. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*destination ipv6 address*>	Specifies the destination address of the test packet. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<*Layer 2 address*>	Specifies the Layer 2 destination address for the test packet using a medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**) or 0xABCDEF format (for example, **1x234567**).
<*target ipv6 address*>	Specifies the IPv6 address of the target neighbor for NS test packets. Specify an IPv6 address in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

Default Values

By default, test packets are not generated for ND messages.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example generates test packets for RA messages on the EVC:

(config)**#system-management-evc**
(config-system-mgmt-evc)**#ipv6 nd generate-packet router-advertisement**

ipv6 nd managed-config-flag

Use the **ipv6 nd managed-config-flag** command to specify the M flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. The M flag instructs hosts receiving the RA that they can use stateful Dynamic Host Configuration Protocol version 6 (DHCPv6) to configure addresses and nonaddress information. Use the **no** form of this command to disable the setting of the M flag.

Syntax Description

No subcommands.

Default Values

By default, the M flag is not set in RAs.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management Ethernet virtual connection (EVC).

Functional Notes

If you specify that the M flag is set in RA messages, you do not need to set the 0 flag (it becomes redundant).

Usage Examples

The following example sets the M flag for RA messages sent by the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd managed-config-flag**

ipv6 nd ns-interval *<value>*

Use the **ipv6 nd ns-interval** command to specify the interval between transmission of certain Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) messages and to control what ND value is advertised in router advertisement (RA) messages. This command is effectual whether the system management Ethernet virtual connection (EVC) is in host or router mode. Use the **no** form of this command to return the interval to the default value.

Syntax Description

<value>	Specifies the time (in milliseconds) between neighbor message transmissions. Valid range is **1000** to **3600000** ms.

Default Values

By default, the interval is set to **1000** ms for internal use by the router and **0** (unspecified) is sent in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

This command controls the spacing of neighbor solicitation (NS) messages for functions such as address resolution, reachability detection, and duplicate address detection (DAD). For DAD it also serves as the amount of time after the last transmission before the detection phase of autoconfiguration terminates. In addition, the command controls the interval between unsolicited neighbor advertisement (NA) messages.

Usage Examples

The following example changes the interval between RA messages sent from the EVC to **2000** ms:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd ns-interval 2000**

ipv6 nd other-config-flag

Use the **ipv6 nd other-config-flag** command to specify the O flag in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the system management Ethernet virtual connection (EVC) is in router mode. When the O flag is set, hosts receiving the RA messages are instructed that they may use stateless Dynamic Host Configuration Protocol version 6 (DHCPv6) to receive information that is not IPv6 addressing information, and to use some other method (whether through manual configuration, stateless address autoconfiguration (SLAAC), etc.) for addressing information. Use the **no** form of this command to disable the O flag setting.

Syntax Description

No subcommands.

Default Values

By default, the O flag is not set in RA messages.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

If the M flag is set for RA messages, you do not need to set the O flag.

Usage Examples

The following example sets the O flag in RA messages from the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd other-config-flag**

ipv6 nd prefix

Use the **ipv6 nd prefix** command to specify the Internet Protocol version 6 (IPv6) address prefixes used in router advertisement (RA) messages sent from the system management Ethernet virtual connection (EVC). Use the **no** form of this command to remove the specified prefix configuration from the EVC. Variations of this command include:

ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite]**
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [no-advertise] [**<*valid lifetime*> | **infinite]** <*preferred lifetime* | **infinite**>
ipv6 nd prefix [named-prefix <*prefix name*>**] [**<*ipv6 prefix/prefix-length*> | **default] [**<*valid lifetime*> | **infinite] [**<*preferred lifetime*> | **infinite] [no-advertise] [no-autoconfig] [no-rtr-address] [no-onlink] [off-link]**

Syntax Description

named-prefix <*prefix name*>	Optional. Specifies that a named prefix is used in RA messages. When a named prefix is used, the default prefix cannot be used.
<*ipv6 prefix/prefix-length*>	Specifies the IPv6 prefix and length to be advertised. Pv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
default	Specifies the default values for the IPv6 prefix parameters. Refer to the *Functional Notes* below for more information.
<*valid lifetime*>	Optional. Specifies the valid lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
<*preferred lifetime*>	Optional. Specifies the preferred lifetime to advertise for this route in each RA message. Range is **0** to **4294967295** seconds.
infinite	Optional. Specifies that the the valid and preferred lifetimes of the prefix do not expire.
no-advertise	Optional. Specifies that the prefix is excluded from the RA message.
no-autoconfig	Optional. Sets the A flag in the RA message to **0**, indicating that hosts may not create an address for this prefix using stateless address autoconfiguration (SLAAC). This parameter only affects hosts receiving the RA message, it does not affect the operation of the local router.
no-rtr-address	Optional. Sets the R flag in the RA message to **0** and specifies the full router IPv6 address is not included in the RA message.
no-onlink	Optional. Specifies that the IPv6 prefix in the RA message is not to be used for on-link determination.
off-link	Optional. Sets the L flag value to **0** in RA messages, which indicates the RA makes no statement about the on-link or off-link properties of the IPv6 prefix.

Default Values

By default, all prefixes derived from the EVC's configured IPv6 addresses are advertised using the system default values.

By default, the valid lifetime advertised for a prefix is **2592000** seconds and the preferred lifetime advertised is **604800** seconds.

By default, the L flag is set to **1**, the R flag is set to **1**, and the A flag is set to **1**.

Command History

Release 18.1	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** and *<prefix name>* options.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

This command works for both routers and hosts, but in host implementations it is used to manually add on-link prefixes that do not have an IPv6 address or to make off-link a prefix generated by an IPv6 address command. Hosts do not send RA messages, so the command only adds prefixes to RA messages when the EVC is in router mode. This command can also be used to change the defaults used on configured prefixes when all options are not specified.

Changing the prefix defaults will affect prefixes derived from configured IPv6 addresses, as well as prefixes configured using the ***ipv6 nd prefix*** *command.*

Prefixes advertised can be a subset or a superset of the prefixes derived from the IPv6 addresses configured on the EVC. Prefixes for IPv6 addresses configured on a router EVC are automatically eligible to be advertised on that interface using system or configured default values without having to enter a prefix command. To impose additional controls on those prefixes, an entry must be made using this command with the desired settings.

The **default** parameter is used to change the default settings for the IPv6 prefix parameters. Changing these settings can be useful when multiple prefixes are implemented that will use the same set of parameters. When configuring IPv6 prefixes, the prefix default values are only used if no other parameters are specified after specifying the IPv6 prefix and length (for example, **ipv6 nd prefix 2001:DB8::/64**). If additional parameters are specified, any unspecified parameters use the system default values rather than the configured default values. When the default values are changed, any prefix that uses them will also change. Using this command to change prefix default values also affects prefixes derived from configured IPv6 addresses on the EVC.

The optional *<valid lifetime>* parameter specifies the valid lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep this prefix until the valid lifetime expires.

The optional <*preferred lifetime*> parameter specifies the preferred lifetime to advertise for this route in each advertisement. Hosts will reset the lifetime to this value each time the route is advertised, and they will keep the prefix in the preferred state during this time period. After the preferred time period expires, the prefix transitions to the deprecated state where it remains until the valid lifetime expires and the route is removed. The <*preferred lifetime*> value must be set to be shorter than the <*valid lifetime*> value.

The optional **off-link** parameter sets the L flag (on-link flag) value to **0** in RA messages. When the L flag is set to 0, the advertisement makes no statement about on-link or off-link properties of the prefix. When the L flag is set, the prefix is considered on-link and locally reachable by hosts on the link (meaning a router is not needed). Hosts attached to the link will add on-link prefixes to their prefix list or route table. When off-link is not specified, a connected route is added to the route table of this router for this prefix. When off-link is specified, no route is added to the route table. By default, prefixes are advertised as on-link with the L flag set to 1.

The optional **no-rtr-address** parameter sets the R flag (router flag) of the RA to **0** and does not include the full router address in the advertisement. The router address is typically included in the RA to assist in Mobile IP environments. By default, the R flag is set to 1 and the router address is sent in RA messages.

The optional **no-autoconfig** parameter sets the A flag of the RA to **0**, indicating that hosts may not create an address for this prefix using SLAAC. If the A flag is set to **1** (the default setting), hosts perform SLAAC to generate an address based on the prefix. This parameter only affects hosts receiving the RA, it does not effect the operation of the local router.

The optional **no-advertise** parameter specifies that the prefix is excluded from RA messages. By default, the prefix is included in RA messages. The **no-onlink** parameter informs the router that the prefix is not to be used for on-link determination.

By default, all prefixes derived from the EVC's configured IPv6 addresses are advertised using the system default values.

Usage Examples

The following example specifies that the IPv6 prefix **2001:DB8:3F::/48** has an infinite valid and preferred lifetime advertised in RA messages sent from the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd prefix 2001:DB8:3F::/48 infinite infinite**

The following example changes the default values and behaviors of prefixes included in RA messages to infinite valid and preferred lifetimes, and specifies that the on- or off-link state of the prefix is not included in the RA and that hosts receiving the RA may not use the prefix for creating an IPv6 address:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd prefix default infinite infinite off-link no-autoconfig**

ipv6 nd purge-timer <*value*>

Use the **ipv6 nd purge-timer** command to specify the maximum amount of time an unused Internet Protocol version 6 (IPv6) neighbor entry remains in the neighbor cache. This command is effectual for the system management Ethernet virtual connection (EVC) in either host or router mode. Use the **no** form of this command to return the purging interval to the default value.

Syntax Description

<*value*>	Specifies the neighbor cache entry storage time in minutes. Valid range is **10** to **1440** minutes.

Default Values

By default, idle (STALE) neighbor cache entries are cleared after **1440** minutes (24 hours).

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

This command applies to EVCs in either router or host mode. A neighbor entry is typically purged when neighbor unreachability detection (NUD) is invoked and the neighbor is determined to no longer be reachable. However, NUD is not performed on idle (STALE) neighbor entries, so this command provides a method for purging unused entries after a specified amount of time.

Usage Examples

The following example specifies that idle neighbor entries in the neighbor cache are removed after **800** minutes:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd purge-timer 800**

ipv6 nd ra interval

Use the **ipv6 nd ra interval** command to specify the interval between transmission of Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the system management Ethernet virtual connection (EVC) is in router mode. Use the **no** form of this command to return to the default value. Variations of this command include:

ipv6 nd ra interval *<max time>*
ipv6 nd ra interval *<max time> <min time>*
ipv6 nd ra interval msec *<max time>*
ipv6 nd ra interval msec *<max time> <min time>*

Syntax Description

<max time>	Specifies the maximum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **4** to **1800** seconds and **70** to **1800000** ms.
<min time>	Optional. Specifies the minimum interval between RA message transmission. Time can be specified in seconds or milliseconds. Range is **3** seconds to 75 percent of the configured maximum time value in seconds, or **30** ms to 75 percent of the configured maximum time value in ms.
msec	Optional. Specifies that the time values are in milliseconds.

Default Values

By default, the interval is set in seconds and has a maximum interval time of **200** seconds and a minimum interval time of 75 percent of the maximum seconds value, but not less than **3** seconds.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

If this router is used as a default router, the interval between RA messages should not be set to a larger value than the RA lifetime set by the command *ipv6 nd ra lifetime <value> on page 3907*, which has a default value of **1800** seconds.

Usage Examples

The following example specifies that the maximum interval in seconds between RA message transmissions is **300**:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#ipv6 nd ra interval 300
```


ipv6 nd ra lifetime <*value*>

Use the **ipv6 nd ra lifetime** command to specify the router lifetime advertised in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command is only effectual when the system management Ethernet virtual connection (EVC) is in router mode. Use the **no** form of this command to return to the default setting. Variations of this command include:

ipv6 nd ra lifetime <*value*>
ipv6 nd ra lifetime default-route

Syntax Description

<*value*>	Specifies the router lifetime in seconds. Range is **0** to **9000** seconds. A value of **0** indicates this is not a default router. A value other than 0 indicates to other nodes that this router can be used as a default router.
default-route	Specifies the RA lifetime is **0** if no default route exists on any IPv6 interface.

Default Values

By default, the router lifetime is set to **1800** seconds.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.
Release R11.5.0	Command was expanded to include the **default-route** parameter.

Functional Notes

A value other than **0** for a router lifetime should be larger than the router advertisement interval specified in the command *ipv6 nd ra interval on page 3906*.

Usage Examples

In the following example, the router lifetime advertised in RA messages is **3000** seconds:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd ra lifetime 3000**

ipv6 nd ra reachable-time *<value>*

Use the **ipv6 nd ra reachable-time** command to specify the value advertised for reachable time in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. This command also specifies the internal base reachable time used by the router. This command is effectual for the system management Ethernet virtual connection (EVC) in either host or router mode. Use the **no** form of this command to return the reachability value to the default setting.

Syntax Description

<value>	Specifies the reachability time in milliseconds. Range is **0** to **3600000** ms. A value of **0** indicates the reachable time is unspecified.

Default Values

By default, the router advertises a reachability time of **0** ms and uses an internal value of **30000** ms.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

This command is effectual for EVCs in either router or host mode. For hosts, this value sets the internal reachable time used by the host if no RAs are received specifying a different value. For routers, the value indicates the amount of time a device is considered reachable after having received a reachability confirmation in neighbor unreachabililty detection (NUD).

Usage Examples

The following example specifies that a reachability time of **50000** ms is advertised in RA messages:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd ra reachable-time 50000**

ipv6 nd ra suppress

Use the **ipv6 nd ra suppress** command to specify whether Internet Protocol version 6 (IPv6) router advertisement (RA) messages will be suppressed. This command is only effectual when the system management Ethernet virtual connection (EVC) in router mode. Use the **no** form of this command to begin sending RA messages.

Syntax Description

No subcommands.

Default Values

By default, RA messages are not suppressed. When IPv6 routing is not enabled on the router, or when implemented in a host-only mode, the default setting is to suppress advertisements on all EVC types.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management EVC.

Usage Examples

The following example suppresses RA messages on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd ra suppress**

ipv6 nd router-preference

Use the **ipv6 nd router-preference** command to specify the default router preference value set in Internet Protocol version 6 (IPv6) router advertisement (RA) messages. Setting this preference helps the receivers of RA messages to determine the preference of one router over another as a default router in environments with multiple routers. Use the **no** form of this command to return the preference to the default setting. Variations of this command include:

ipv6 nd router-preference high
ipv6 nd router-preference low
ipv6 nd router-preference medium

Syntax Description

high	Specifies the preference value is high.
low	Specifies the preference value is low.
medium	Specifies the preference value is medium.

Default Values

By default, the router preference is set to medium.

Command History

Release 18.1	Command was introduced.
Release R10.10.0	Command was expanded to include the system management Ethernet virtual connection (EVC).

Usage Examples

The following example specifies that the advertised default router preference is high:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 nd router-preference high**

ipv6 route-cache

Use the **ipv6 route-cache** command to enable Internet Protocol version 6 (IPv6) fast-cache switching on the system management Ethernet virtual connection (EVC). Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay subinterfaces. IP route cache is enabled for all virtual Point-to-Point Protocol (PPP) interfaces.

Command History

Release 18.2	Command was introduced.
Release R10.7.0	Command was expanded to include the tunnel interface.
Release R10.10.0	Command was expanded to include the system management EVC.

Functional Notes

Fast switching allows an EVC to provide optimum performance when processing IPv6 traffic.

Usage Examples

The following example enables IPv6 fast switching on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#ipv6 route-cache**

max-reserved-bandwidth *<value>*

Use the **max-reserved-bandwidth** command to specify the percentage of interface bandwidth reserved for use in user-defined (priority or class-based) queues. The remainder of the interface bandwidth is reserved for system-critical traffic and is not available to user-defined queues. Use the **no** form of this command to restore the default value.

Reserving a portion of the interface bandwidth for system-critical traffic is necessary for proper operation. Specifying the entire interface bandwidth for use in user-defined queues can cause undesirable operation.

Syntax Description

<value>	Specifies the maximum percentage of bandwidth to reserve for quality of service (QoS). This setting is configured as a percentage of the total interface speed. Range is **1** to **100** percent.

Default Values

By default, **max-reserved-bandwidth** is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical traffic.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was expanded to include the bridged virtual interfaces (BVIs).
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet subinterface.
Release R11.1.0	Command was expanded to include the system management Ethernet virtual connection (EVC) and the system control EVC.

Usage Examples

The following example specifies **85** percent of the bandwidth on the system management EVC be available for use in user-defined queues:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#max-reserved-bandwidth 85**

men-pri

Use the **men-pri** command to specify the default value of the S-tag used in the system management Ethernet virtual connection (EVC) communication. Use the **no** form of this command to return to the default setting. Variations of this command include:

men-pri inherit
men-pri <*value*>

Syntax Description

inherit	Specifies that the S-tag priority value is inherited from the customer equipment (CE) virtual local area network (VLAN).
<*value*>	Specifies a priority value for the S-tag. Valid range is **0** to **7**.

Default Values

By default, the S-tag is set to **inherit**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that the S-tag has a priority of **5** on the EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#men-pri 5**

qos-policy

Use the **qos-policy** command to apply a previously configured quality of service (QoS) map to incoming or outgoing packets on an interface. Use the **no** form of this command to remove the map from the interface. Variations of this command include:

qos-policy in <*name*>
qos-policy out <*name*>

Syntax Description

<*name*>	Specifies the name of a previously created QoS map (refer to *qos map <name> <number> on page 1673* for more information).
in	Assigns a QoS map to this interface's input.
out	Assigns a QoS map to this interface's output.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.
Release 15.1	Command was expanded to include the **in** parameter.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the system control Ethernet virtual connection (EVC) and system management EVC.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair queue to use weighted fair queuing.
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when asymmetric digital subscriber line (ADSL) finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the system management EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#qos-policy out VOICEMAP**

rtp quality-monitoring

Use the **rtp quality-monitoring** command to enable voice quality monitoring (VQM) of the Realtime Transport Protocol (RTP) voice stream packets on this interface. If the global command (**ip rtp quality-monitoring**) is disabled when this command is issued, the system will return the following warning: "Applied but not used, you must globally enable **ip rtp quality-monitoring** to use VQM." Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, VQM is enabled on all wide area network (WAN) and local area network (LAN) interfaces.

Command History

Release 17.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet interface.
Release R11.2.0	Command was expanded to include the system control Ethernet virtual connection (EVC) and system management EVC.

Usage Examples

The following example enables RTP quality monitoring on the system management EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#rtp quality-monitoring**

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface. Us the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and subinterfaces) have SNMP traps enabled.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the port channel and virtual local area network (VLAN) interfaces.
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Usage Examples

The following example enables SNMP capability on the system management EVC:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#snmp trap
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC 2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable object identifier (OID) is enabled for all interfaces except virtual Frame Relay interfaces.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the Ethernet subinterfaces and Gigabit Ethernet interfaces.
Release 6.1	Command was expanded to include the E1, port channel, T3, and virtual local area network (VLAN) interfaces.
Release 7.1	Command was expanded to the high speed serial interface (HSSI).
Release 8.1	Command was expanded to the asynchronous transfer mode (ATM) interface.
Release 9.1	Command was expanded to the high level data link control (HDLC) interface.
Release 11.1	Command was expanded to the demand interface.
Release 16.1	Command was expanded to the tunnel interface.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the single-pair high-speed digital subscriber line (SHDSL) interface, Ethernet in the first mile (EFM) group, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the system management EVC:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#no snmp trap link-status**

s-tag

Use the **s-tag** command to specify the virtual local area network (VLAN) ID used by the service provider for the system management Ethernet virtual connection (EVC). This VLAN ID, the s-tag, is used by the carrier to mark outbound traffic from this EVC in the Metro Ethernet network (MEN). Use the **no** form of this command to return the s-tag value to the default. Variations of this command include:

s-tag <*vlan id*>
s-tag none

Syntax Description

<*vlan id*>	Specifies ID of the service provider VLAN. Valid range is **1** to **4094**.
none	Specifies no S-tag is used.

Default Values

By default, the s-tag is **0**, which indicates the traffic on the EVC is untagged.

Command History

Release A3.01	Command was introduced.
Release R10.10.0	Command was expanded to include the **none** parameter and the system management EVC.

Usage Examples

The following example specifies the s-tag for traffic outbound on the EVC is **20**:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#s-tag 20**

traffic-shape rate *<value>*

Use the **traffic-shape rate** command to specify and enforce an output bandwidth for the system management Ethernet virtual connection (EVC). Variations of this command include:

traffic-shape rate *<value>*
traffic-shape rate *<value>* **count-eth-overhead**
traffic-shape rate *<value>* *<burst>*
traffic-shape rate *<value>* *<burst>* **count-eth-overhead**

Syntax Description

<value>	Specifies the rate (in bits per second) at which the interface should be shaped.
<burst>	Optional. Specifies the allowed burst in bytes. By default, the burst is specified as the rate divided by 5 and represents the number of bytes that would flow within 200 ms.
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.

Default Values

By default, traffic-shaping rate is disabled.

Command History

Release 10.1	Command was introduced.
Release A3.01	Command was expanded to include the Metro Ethernet Forum (MEF) Ethernet Interface.
Release R11.1.0	Command was expanded to include the **count-eth-overhead** parameter, system management Ethernet virtual connection (EVC) and the system control EVC.

Functional Notes

Traffic shaping can be used to limit an Ethernet segment to a particular rate or to specify use of quality of service (QoS) on Ethernet or VLAN interfaces.

Usage Examples

The following example sets the outbound rate of traffic on the system management EVC to 128 kbps:

(config)**#system-management-evc**
(config-sys-mgmt-evc)**#traffic-shape rate 128000**

vrf forwarding <*name*>

Use the **vrf forwarding** command to assign an Ethernet virtual connection (EVC) to a specific virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the EVC from the named VRF instance and assign it to the unnamed default VRF.

Keep in mind that changing an EVC's VRF association will clear all IP-related settings on that EVC.

Syntax Description

<name>	Specifies the name of the VRF to which to assign the EVC.

Default Values

By default, EVCs are associated with the default VRF that is unnumbered.

Command History

Release 16.1	Command was introduced.
Release 17.8	The keyword **ip** was removed from this command.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.

Functional Notes

VRF instances must be created first before an EVC can be assigned. An EVC can only be assigned to one VRF, but multiple EVCs can be assigned to the same VRF.

An EVC will only forward IP traffic that matches its associated VRF.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example assigns the system control EVC to the VRF instance named **RED**:

(config)**#system-control-evc**
(config-sys-cntrl-evc)**#vrf forwarding RED**

Y.1731 COMMAND SETS

This section includes the following command sets:

ONE-WAY FRAME DELAY MONITORING SESSION COMMAND SET

A one-way frame delay performance monitoring session can be configured to run between any two Y.1731 maintenance entity group (MEG) endpoints (MEPs). This session monitors frame delays in a one way transmission between a source MEP and a target MEP. The source MEP sends a one-way delay measurement message (1DM) frame to the target MEP, which terminates the 1DM and calculates the one-way frame delay. Two timestamps are used for one-way frame delay messaging. The source MEP applies a transmit timestamp to the outgoing 1DM frame and the target MEP applies a receive timestamp upon receiving the 1DM frame.

A local MEP can run several one-way frame delay performance monitoring sessions between itself and the target MEP as long as each session uses a different priority value. This allows the target MEP to simultaneously monitor frame delay performance at different classes of service. If the two MEPs are synchronized based on the time of day, the following measurements can be performed:

- Minimum one-way frame delay
- Maximum one-way frame delay
- Mean one-way frame delay
- Maximum one-way frame delay variation (reference packet)
- Maximum one-way frame delay variation (inter-packet)

The one-way frame delay command set is used to configure the transmit attributes of the one-way frame delay performance monitoring session. The One-way Frame Delay Configuration mode is accessed from the Local MEP Configuration mode (refer to *Y.1731 Local MEP Command Set on page 3950*) using the **frame-delay one-way** <*mep id* | *target mac address*> **priority** <*value*> command. To access this configuration mode, enter the command as follows:

```
(config)#ethernet y1731 meg char-string MEG1 level 3
(config-y1731-meg MEG1)#local-mep 3
MEP 3 created
(config-y1731-mep3)#frame-delay one-way 500 priority 1
(config-y1731-frame-delay)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide:

cross-connect on page 76
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

data <data> on page 3924
interval <interval> on page 3925
size <bytes> on page 3926

data <*data*>

Use the **data** command to set the transmit data pattern for the one-way frame delay monitoring session. Use the **no** form of this command to return to the default value.

Syntax Description

<*data*>	Specifies the hexadecimal pattern used to fill the data type-length value (TLV). Valid range is **0x0000** to **0xFFFF**.

Default Values

By default, the data pattern is set to **0x0000**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example sets the transmit data pattern for the one-way frame delay monitoring session to **0x1111**:

(config-y1731-mep3)**#frame-delay one-way 500 priority 1**
(config-y1731-frame-delay)**#data 0x1111**

interval *<interval>*

Use the **interval** command to specify the time in milliseconds between one-way delay measurement message (1DM) transmissions. Use the **no** form of this command to return to the default value.

Syntax Description

<interval>	Specifies the time in milliseconds between 1DM transmissions. Valid range is **100** to **10000** ms.

Default Values

By default, the interval is set to **1000** ms.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies the interval between 1DM transmissions is **3500** ms:

(config-y1731-mep3)**#frame-delay one-way 500 priority 1**
(config-y1731-frame-delay)**#interval 3500**

size <*bytes*>

Use the **size** command to specify the size of the one-way delay measurement message (1DM) frame. Use the **no** form of this command to return to the default value.

Syntax Description

<*bytes*>	Specifies the size of the 1DM frame. If no size is specified, 1DM frames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the 1DM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.

Default Values

By default, the size is set to **0** bytes.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example sets the size of the 1DM frame to **100** bytes:

(config-y1731-mep3)**#frame-delay one-way 500 priority 1**
(config-y1731-frame-delay)**#size 100**

TWO-WAY FRAME DELAY MONITORING SESSION COMMAND SET

A two-way frame delay performance monitoring session can be configured to run between any two Y.1731 maintenance entity group (MEG) endpoints (MEPs). This session monitors frame delays in a two-way transmission between a source MEP and a target MEP. The source MEP sends a delay measurement message (DMM) to the target MEP, which replies with a delay measurement reply (DMR). Four timestamps are used for two-way frame delay messaging. In this process, the target MEP applies timestamps to the DMR frame indicating its arrival and transmission time. The source MEP then removes the processing time at the target MEP and only measures the time the DMM/DMR frame was on the wire.

A local MEP can run several two-way frame delay performance monitoring sessions between itself and the target MEP as long as each session uses a different priority value. This allows the target MEP to simultaneously monitor frame delay performance at different classes of service. The two-way frame delay monitoring session can monitor the following metrics:

- Minimum two-way frame delay
- Maximum two-way frame delay
- Mean two-way frame delay
- Maximum two-way frame delay variation (reference packet)
- Maximum two-way frame delay variation (inter-packet)

If the two MEPs are synchronized based on the time of day, the following additional measurements can be performed in both egress and ingress directions:

- Minimum one-way frame delay
- Maximum one-way frame delay
- Mean one-way frame delay

The two-way frame delay command set is used to configure the transmit attributes of the two-way frame delay performance monitoring session. The Two-Way Frame Delay Configuration mode is accessed from the Local MEP Configuration mode (refer to *Y.1731 Local MEP Command Set on page 3950*) using the **frame-delay two-way** <*mep id* | *target mac address*> **priority** <*value*> command. To access this configuration mode, enter the command as follows:

```
(config)#ethernet y1731 meg char-string MEG1 level 3
(config-y1731-meg MEG1)#local-mep 3
MEP 3 created
(config-y1731-mep3)#frame-delay two-way 500 priority 1
(config-y1731-frame-delay)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide:

cross-connect on page 76
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

bulk-data-export

Use the **bulk-data-export** command to determine which, if any, files are generated by the delay measurement message (DMM) performance monitoring session. The files are used to store two-way frame delay statistics. Use the **no** form of this command to disable the bulk data export feature. Variations of this command include:

bulk-data-export averaged
bulk-data-export none

Syntax Description

averaged	Specifies that statistics generated by each measurement interval are stored. Measurement intervals are specified using the command *measurement-interval on page 3932*.
none	Specifies that no statistics are stored.

Default Values

By default, no statistics are stored.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that statistics generated by each measurement interval are stored:

(config-y1731-mep3)**#frame-delay two-way 500 priority 1**
(config-y1731-frame-delay)**#bulk-data-export averaged**

data *<data>*

Use the **data** command to set the transmit data pattern for the two-way frame delay monitoring session. Use the **no** form of this command to return to the default value.

Syntax Description

<data>	Specifies the hexadecimal pattern used to fill the data type-length value (TLV). Valid range is **0x0000** to **0xFFFF**.

Default Values

By default, the data pattern is set to **0x0000**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example sets the transmit data pattern for the two-way frame delay monitoring session to **0x1111**:

(config-y1731-mep3)**#frame-delay two-way 500 priority 1**
(config-y1731-frame-delay)**#data 0x1111**

interval *<interval>*

Use the **interval** command to specify the time in milliseconds between delay measurement message (DMM) transmissions. Use the **no** form of this command to return to the default value.

Syntax Description

<interval>	Specifies the time in milliseconds between DMM transmissions. Valid range is **100** to **10000** ms.

Default Values

By default, the interval is set to **1000** ms.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies the interval between DMM transmissions is **3500** ms:

(config-y1731-mep3)**#frame-delay two-way 500 priority 1**
(config-y1731-frame-delay)**#interval 3500**

measurement-interval

Use the **measurement-interval** command to specify the interval over which two-way frame delay statistics are generated. The statistics calculated for a measurement interval are stored in the averaged data file (refer to the command *bulk-data-export on page 3929*). Use the **no** form of this command to return to the default setting.

measurement-interval <*measurement interval*>
measurement-interval <*measurement interval*> <*repetition time*>
measurement-interval <*measurement interval*> **none**

Syntax Description

<*measurement interval*>	Specifies the number of seconds over which frame delay statistics are generated. If used with the <*repetition-time*> variable, must be in minute intervals (multiples of 60) and less than the repetition time. Valid range is **60** to **86400** seconds.
<*repetition time*>	Specifies the number of seconds between the start time of measurement intervals. The repetition time must be at least as long as the measurement interval and must be in minute intervals (multiples of 60). Valid range is **60** to **86400** seconds.
none	Specifies that the repetition time is equal to the measurement interval.

Default Values

By default, the measurement interval is set to **60** seconds and the repetition time is set to **none**.

Command History

Release R10.10.0	Command was introduced.
Release R11.6.0	Command was expanded to include the <*repetition time*> variable and the **none** parameter.

Usage Examples

The following example specifies the measurement interval is **120** seconds and the repetition time is **240**:

(config-y1731-mep3)**#frame-delay two-way 500 priority 1**
(config-y1731-frame-delay)**#measurement-interval 120 240**

size <*bytes*>

Use the **size** command to specify the size of the delay measurement message (DMM) frame. Use the **no** form of this command to return to the default value.

Syntax Description

<*bytes*>	Specifies the size of the DMM frame. If no size is specified, DMM frames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the DMM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.

Default Values

By default, the size is set to **0** bytes.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example sets the size of the DMM frame to **100** bytes:

(config-y1731-mep3)**#frame-delay two-way 500 priority 1**
(config-y1731-frame-delay)**#size 100**

stop-time

Use the **stop-time** command to specify the duration of the frame delay monitoring session (in seconds). This is how long the frame delay monitoring session will run after the session begins. Use the **no** form of this command to return to the default value. Variations of this command include:

stop-time <*stop-time*>
stop-time forever

Syntax Description

<*stop-time*>	Specifies the duration in seconds of the frame delay monitoring session. Valid range is **0** to **15552000** seconds.
forever	Specifies that the frame delay monitoring session will continue until it is manually stopped.

Default Values

By default, the **stop-time** is set to **forever**.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example specifies a monitoring session duration of **3600** seconds:

(config-y1731-mep3)**#frame-loss synthetic single-ended 500 priority 1**
(config-y1731-frame-delay)**#stop-time 3600**

SINGLE-ENDED FRAME LOSS MONITORING SESSION COMMAND SET

In Y.1731, the Ethernet Loss Measurement Function (ETH-LM) can be used to monitor frame loss across a service by counting in-profile customer frames. This protocol operates in a single-ended mode in which one maintenance entity group (MEG) endpoint (MEP) initiates a session and sends a request to a peer MEP which sends a response. These sessions can be executed between any two MEPs in the same MEG.

During a session, a loss measurement message (LMM) is sent from the source MEP to the target MEP, which replies with a loss measurement reply (LMR). In this process, each MEP maintains a set of two counters that count the frames transmitted towards the target MEP and the frames received from that MEP. These counters increment when in-profile frames (those that are green or received with the drop eligible indicator (DEI) bit set to false) are transmitted and received. Frames counted in this process are only data frames, and not LMM or LMR frames.

A local MEP can run several single-ended frame loss performance monitoring sessions between itself and a target MEP as long as each session uses a different priority value. This allows the MEP to simultaneously monitor frame loss performance at different classes of service.

The Single-Ended Frame Loss Configuration mode is accessed from the Local MEP Configuration mode using the command *frame-loss single-ended on page 3960*. To access this configuration mode, enter the command from the Local MEP Configuration mode as shown in the following example:

```
(config)#ethernet y1731 meg char-string MEG1 level 4
(config-y1731-meg MEG1)#local-mep 3
(config-y1731-mep3)#frame-loss single-ended 500 priority 1
(config-y1731-frame-loss)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide:

cross-connect on page 76
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

data <*data*>

Use the **data** command to set the transmit data pattern for the single-ended frame loss monitoring session. Use the **no** form of this command to return to the default value.

Syntax Description

<*data*>	Specifies the hexadecimal pattern used to fill the data type-length value (TLV). Valid range is **0x0000** to **0xFFFF**.

Default Values

By default, the data pattern is set to **0x0000**.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example sets the transmit data pattern for the frame loss monitoring session to **0x1111**:

(config-y1731-mep3)**#frame-loss single-ended 500 priority 1**
(config-y1731-frame-loss)**#data 0x1111**

interval *<interval>*

Use the **interval** command to specify the time in milliseconds between loss measurement message (LMM) transmissions. Use the **no** form of this command to return to the default value.

Syntax Description

<interval>	Specifies the time in milliseconds between LMM transmissions. Valid range is **100** to **900000** ms.

Default Values

By default, the interval is set to **1000** ms.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example specifies the interval between LMM transmissions is **3500** ms:

(config-y1731-mep3)**#frame-loss single-ended 500 priority 1**
(config-y1731-frame-loss)**#interval 3500**

measurement-interval

Use the **measurement-interval** command to specify the interval over which frame loss statistics are generated. Use the **no** form of this command to return to the default setting.

measurement-interval <*measurement interval*>
measurement-interval <*measurement interval*> <*repetition time*>
measurement-interval <*measurement interval*> **none**

Syntax Description

<*measurement interval*>	Specifies the number of seconds over which frame loss statistics are generated. If used with the <*repetition-time*> variable, must be in minute intervals (multiples of 60) and less than the repetition time. Valid range is **60** to **86400** seconds.
<*repetition time*>	Specifies the number of seconds between the start time of measurement intervals. The repetition time must be at least as long as the measurement interval and must be in minute intervals (multiples of 60). Valid range is **60** to **86400** seconds.
none	Specifies that the repetition time is equal to the measurement interval.

Default Values

By default, the measurement interval is set to **60** seconds and the repetition time is set to **none**.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example specifies the measurement interval is **120** seconds and the repetition time is **240**:

(config-y1731-mep3)**#frame-loss single-ended 500 priority 1**
(config-y1731-frame-loss)**#measurement-interval 120 240**

size <*size*>

Use the **size** command to specify the size of the loss measurement message (LMM) frame. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Specifies the size in bytes of the LMM frame. If no size is specified, LMM frames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the LMM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.

Default Values

By default, the size is set to **0** bytes.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example sets the size of the LMM frame to **100** bytes:

(config-y1731-mep3)**#frame-loss single-ended 500 priority 1**
(config-y1731-frame-loss)**#size 100**

stop-time

Use the **stop-time** command to specify the duration of the frame loss monitoring session (in seconds). This is how long the frame loss monitoring session will run after the session begins. Use the **no** form of this command to return to the default value. Variations of this command include:

stop-time <*stop-time*>
stop-time forever

Syntax Description

<*stop-time*>	Specifies the duration in seconds of the frame loss monitoring session. Valid range is **0** to **15552000** seconds.
forever	Specifies that the frame loss monitoring session will continue until it is manually stopped.

Default Values

By default, the **stop-time** is set to **forever**.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example specifies a monitoring session duration of **3600** seconds:

(config-y1731-mep3)**#frame-loss single-ended 500 priority 1**
(config-y1731-frame-loss)**#stop-time 3600**

SINGLE-ENDED SYNTHETIC FRAME LOSS MONITORING SESSION COMMAND SET

In Y.1731, the Ethernet Loss Measurement Function (ETH-SLM) can be used to monitor frame loss across a service by counting synthetic data frames. This protocol operates in a single-ended mode in which one maintenance entity group (MEG) endpoint (MEP) initiates a session and sends a request to a peer MEP which sends a response. These sessions can be executed between any two MEPs in the same MEG.

During a session, a synthetic loss message (SLM) is sent from the source MEP to the target MEP, which replies with a synthetic loss reply (SLR). In this process, each MEP maintains a set of two counters that count the frames transmitted towards the target MEP and the frames received from that MEP. These counters increment when the synthetic frames are transmitted and received. Frames counted in this process are SLM and SLR frames, not actual data frames.

A local MEP can run several single-ended frame loss performance monitoring sessions between itself and a target MEP as long as each session uses a different priority value. This allows the MEP to simultaneously monitor frame loss performance at different classes of service. g measurement interval

The Single-Ended Synthetic Frame Loss Configuration mode is accessed from the Local MEP Configuration mode using the command *frame-loss synthetic single-ended on page 3963*. To access this configuration mode, enter the command from the Local MEP Configuration mode as shown in the following example:

```
(config)#ethernet y1731 meg char-string MEG1 level 4
(config-y1731-meg MEG1)#local-mep 3
(config-y1731-mep3)#frame-loss synthetic single-ended 500 priority 1
(config-y1731-syn-frame-loss)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide:

cross-connect on page 76
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

bulk-data-export

Use the **bulk-data-export** command to determine which, if any, files are generated by the synthetic loss message (SLM) performance monitoring session. The files are used to store two-way frame delay statistics. Use the **no** form of this command to disable the bulk data export feature. Variations of this command include:

bulk-data-export averaged
bulk-data-export none

Syntax Description

averaged	Specifies that statistics generated by each measurement interval are stored. Measurement intervals are specified using the command *measurement-interval on page 3947*.
none	Specifies that no statistics are stored.

Default Values

By default, no statistics are stored.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that statistics generated by each measurement interval are stored:

(config-y1731-mep3)**#frame-loss synthetic single-ended 500 priority 1**
(config-y1731-syn-frame-loss)**#bulk-data-export averaged**

data *<data>*

Use the **data** command to set the transmit data pattern for the single-ended frame loss monitoring session. Use the **no** form of this command to return to the default value.

Syntax Description

<data>	Specifies the hexadecimal pattern used to fill the data type-length value (TLV). Valid range is **0x0000** to **0xFFFF**.

Default Values

By default, the data pattern is set to **0x0000**.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example sets the transmit data pattern for the frame loss monitoring session to **0x1111**:

(config-y1731-mep3)**#frame-loss synthetic single-ended 500 priority 1**
(config-y1731-syn-frame-loss)**#data 0x1111**

interval *<interval>*

Use the **interval** command to specify the time in milliseconds between synthetic loss message (SLM) transmissions. Use the **no** form of this command to return to the default value.

Syntax Description

<interval>	Specifies the time in milliseconds between SLM transmissions. Valid range is **100** to **900000** ms.

Default Values

By default, the interval is set to **1000** ms.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies the interval between SLM transmissions is **3500** ms:

```
(config-y1731-mep3)#frame-loss synthetic single-ended 500 priority 1
(config-y1731-syn-frame-loss)#interval 3500
```

measurement-interval

Use the **measurement-interval** command to specify the interval over which frame loss statistics are generated. The statistics calculated for a measurement interval are stored in the averaged data file (refer to the command *bulk-data-export on page 3944*). Use the **no** form of this command to return to the default setting. Variations of this command include:

measurement-interval <*measurement interval*>
measurement-interval <*measurement interval*> <*repetition time*>
measurement-interval <*measurement interval*> **none**

Syntax Description

<*measurement interval*>	Specifies the number of seconds over which frame loss statistics are generated. If used with the <*repetition-time*> variable, must be in minute intervals (multiples of 60) and less than the repetition time. Valid range is **60** to **86400** seconds.
<*repetition time*>	Specifies the number of seconds between the start time of measurement intervals. The repetition time must be at least as long as the measurement interval and must be in minute intervals (multiples of 60). Valid range is **60** to **86400** seconds.
none	Specifies that the repetition time is equal to the measurement interval.

Default Values

By default, the measurement interval is set to **60** seconds and the repetition time is set to **none**.

Command History

Release R10.10.0	Command was introduced.
Release R11.6.0	Command was expanded to include the <*repetition time*> variable and the **none** parameter.

Usage Examples

The following example specifies the measurement interval is **120** seconds and the repetition time is **240**:

(config-y1731-mep3)**#frame-loss synthetic single-ended 500 priority 1**
(config-y1731-syn-frame-loss)**#measurement-interval 120 240**

size <*size*>

Use the **size** command to specify the size of the synthetic loss message (SLM) frame. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*>	Specifies the size in bytes of the SLM frame. If no size is specified, SLM frames are zero-padded up to 64 bytes. If the size is specified, a data type-length value (TLV) is used to ensure the SLM frame is the correct length. Valid range is **0**, or **64** to **2000** bytes.

Default Values

By default, the size is set to **0** bytes.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example sets the size of the SLM frame to **100** bytes:

(config-y1731-mep3)**#frame-loss synthetic single-ended 500 priority 1**
(config-y1731-syn-frame-loss)**#size 100**

stop-time

Use the **stop-time** command to specify the duration of the frame loss monitoring session (in seconds). This is how long the frame loss monitoring session will run after the session begins. Use the **no** form of this command to return to the default value. Variations of this command include:

stop-time <*stop-time*>
stop-time forever

Syntax Description

<*stop-time*>	Specifies the duration in seconds of the frame loss monitoring session. Valid range is **0** to **15552000** seconds.
forever	Specifies that the frame loss monitoring session will continue until it is manually stopped.

Default Values

By default, the **stop-time** is set to **forever**.

Command History

Release R11.6.0	Command was introduced.

Usage Examples

The following example specifies a monitoring session duration of **3600** seconds:

(config-y1731-mep3)**#frame-loss synthetic single-ended 500 priority 1**
(config-y1731-syn-frame-loss)**#stop-time 3600**

Y.1731 Local MEP Command Set

A maintenance entity group end point (MEP) is a connectivity fault management (CFM) entity that is implemented at the ends of a maintenance entity (ME) which generates and receives CFM protocol data units (PDUs). MEPs drop, pass, or process CFM packets ingressing on the ports to which they are assigned. If the ingressing CFM packets have a lower maintenance level than the MEP, the packets are dropped. If the MEP receives CFM packets that have a higher maintenance level, the packets are passed transparently. CFM packets with a maintenance domain equal to the MEP are processed. MEPs also ensure the continuity of the maintenance association (MA) to which they belong by periodically transmitting continuity check messages (CCMs) to other MEPs in the MA.

To access the Y.1731 local MEP command set, enter the **local-mep** <*id*> command from the Y.1731 MEG configuration mode prompt, and then enter the appropriate Y.1731 application command as follows (refer to the command *local-mep <id> on page 3970*):

```
(config)#ethernet y1731 meg char-string MEG1 level 1
(config-y1731-meg MEG1)#local-mep 3
MEP 3 created
(config-y1731-mep3)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

ccm frame-loss on page 3951
ccm-enabled on page 3952
ccm-enabled track <name> on page 3953
direction on page 3954
force-rdi track <name> on page 3955
frame-delay one-way on page 3956
frame-delay two-way on page 3957
frame-delay two-way file-save averaged on page 3958
frame-loss single-ended on page 3960
frame-loss single-ended file-save averaged on page 3961
frame-loss synthetic single-ended on page 3963
frame-loss synthetic single-ended file-save averaged on page 3964
priority <value> on page 3966
set interface on page 3967

ccm frame-loss

Use the **ccm frame-loss** command to configure the method used to calculate frame loss using received continuity check message (CCM) protocol data units (PDUs). Use the **no** form of this command to return to the default setting. Variations of this command include:

ccm frame-loss measurement-interval <*seconds*>
ccm frame-loss sequence-number

Syntax Description

measurement interval <*seconds*>	Specifies the interval over which frame loss statistics are generated. Valid range is **60** to **900** seconds.
sequence-number	Specifies that frame loss is calculated using the sequence number in CCMs.

Default Values

By default, CCMs do not use a sequence number for calculating frame loss measurements, and the default measurement interval is **60** seconds.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example configures frame loss to be calculated using the sequence number in the CCMs:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#ccm frame-loss sequence-number**

ccm-enabled

Use the **ccm-enabled** command to enable transmission of continuity check message (CCM) frames by the maintenance entity group end point (MEP). Use the **no** form of this command to disable CCMs.

Syntax Description

No subcommands.

Default Values

By default, CCMs are disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables transmission of CCM frames:

```
(config-y1731-meg MEG1)#local-mep 3
MEP 3 created
(config-y1731-mep3)#ccm-enabled
```

ccm-enabled track *<name>*

Use the **ccm-enabled track** command to enable transmission of continuity check message (CCM) frames while the specified track is in the PASS state. While the specified track is in the FAIL state, the local MEP will not send CCMs.

Syntax Description

<name>	Specifies the name of the track on which to base CCM frame transmission.

Default Values

By default, CCM transmission is disabled.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example enables transmission of CCM frames on the local MEP when the track **EXAMPLE_TRACK** is in the PASS state:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#ccm-enabled track EXAMPLE_TRACK**

direction

Use the **direction** command to specify the direction that the active side of the maintenance entity group end point (MEP) will be pointing in relation to the switch. The direction must be specified to activate the MEP. Use the **no** form of this command to return to the default setting. Variations of this command include:

direction down
direction up

Syntax Description

down	Specifies that the MEP will receive and transmit frames on the interface without accessing the switch.
up	Specifies that the MEP will receive and transmit frames towards the switch without accessing the interface.

Default Values

By default, the direction of the MEP is unspecified.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that the MEP will receive and transmit frames towards the switch without accessing the interface:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#direction up**

force-rdi track <*name*>

Use the **force-rdi track** command to specify that the maintenance entity group end point (MEP) should force the transmission of remote defect indications (RDIs) while the track is in the PASS state, and should transmit RDIs according to the rules of Y.1731 when the track is in the FAIL state. This connects the MEP's RDI transmission to the administrative state of the user-network interface (UNI) or network-to-network interface (NNI). Use the **no** form of this command to remove the association between the track's state and the MEP's RDI transmission.

Syntax Description

<*name*>	Specifies the name of the track that should control the transmission of RDIs on the MEP.

Default Values

By default, RDIs are transmitted according to the rules of Y.1731.

Command History

Release R11.5.0	Command was added.

Usage Examples

The following example specifies that the RDI transmission of MEP **3** should be controlled by the track **GIG_3_OPER_STATUS**:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#force-rdi track GIG_3_OPER_STATUS**

frame-delay one-way

Use the **frame-delay one-way** command to configure a Y.1731 one-way frame delay performance monitoring session between maintenance entity group (MEG) endpoints (MEPs). Use the **no** form of this command to disable the frame delay monitoring session. Variations of this command include:

frame-delay one-way measurement-interval
frame-delay one-way <*mep id* > **priority** <*value*>
frame-delay one-way <*target mac address*> **priority** <*value*>
frame-delay one-way multicast priority <*value*>

Syntax Description

measurement-interval	Specifies the interval over which frame delay statistics are generated. Valid range is **60** to **900** seconds.
<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191**.
<*target mac address*>	Specifies the medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
priority <*value*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.

Default Values

By default, no one-way frame delay monitoring sessions are configured. If a session is configured, by default it has a measurement interval of **60** seconds.

Command History

Release R10.10.0	Command was introduced.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a one-way frame delay monitoring session for MEP **100** with a priority of **3**:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#frame-delay one-way 100 priority 3**

frame-delay two-way

Use the **frame-delay two-way** command to configure a Y.1731 two-way frame delay performance monitoring session between maintenance entity group (MEG) endpoints (MEPs). Use the **no** form of this command to disable the frame delay monitoring session. Variations of this command include:

frame-delay two-way <*mep id*> **priority** <*value*>
frame-delay two-way <*target mac address*> **priority** <*value*>
frame-delay two-way multicast priority <*value*>

Syntax Description

<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191**.
<*target mac address*>	Specifies the medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
priority <*value*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.

Default Values

By default, no two-way frame delay monitoring sessions are configured. If a session is configured, by default it has a measurement interval of **60** seconds.

Command History

Release R10.10.0	Command was introduced.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a two-way frame delay monitoring session for MEP **100** with a priority of **3**:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#frame-delay two-way 100 priority 3**

frame-delay two-way file-save averaged

Use the **frame-delay two-way file-save averaged** command to specify that averaged two-way frame delay (ETH-DM) measurement interval data is saved to performance monitoring logs. Use the **no** form of this command to disable saving data to the performance monitoring logs.

Syntax Description

No subcommands.

Default Values

By default, the ETH-DM measurement interval data is not saved to the performance monitoring logs.

Command History

Release 11.6.0	Command was introduced.

Functional Notes

By default, each time a new measurement interval occurs during a Y.1731 performance monitoring session, ETH-DM, ETH-LM, and ETH-SLM, the data from the previous interval is overwritten. The performance monitoring file save feature allows performance monitoring logs to be stored in memory in a series of hour-long log files. The unit records session data to the current log file at user-specified intervals. At the end of the user-specified log lifetime, the logs are rotated out in a first-in first-out fashion; the oldest files are deleted to make room for the new files. Each performance monitoring session type is stored in a separate file in the user-specified directory. The file is automatically named by the unit using the following format:

<*device serial*>**_<DM | LM | SLM>.Data_**<*date and time*>**.pm.xz[.current]**

Parameter	Description
<*device serial*>	Specifies the serial number of the unit.
DM	Specifies that the file is a single-ended (two-way) frame delay log.
LM	Specifies that the file is a single-ended frame loss log.
SLM	Specifies that the file is a single-ended synthetic frame loss log.
<*date and time*>	Specifes the date and time at which the log ends in the format **YYYY-MM-DD_hh.mm.ss**, for example: **2014-12-30_14:00:00**. This specifies the last time interval that the file will be written.
.pm.xz	Specifies the file extension of the log file.
.current	Appended to files that are still in use and could have data written to them.

The following example is a sample ETH-SLM file name that is no longer writable:

LBADTN340767_SLM.Data_2014-12-04_15.00.00.pm.xz

The following example is a sample ETH-LM file name of a file to which the unit is currently writing:

LBADTN340767_LM.Data_2014-12-04_15.00.00.pm.xz.current

If the file directory for the log files is changed, the files in the previous save directory will not be deleted for log rotation. Log rotation only occurs for files in the currently-specified save directory.

If any of the following conditions occur during a measurement interval, the measurement will be considered suspect, and it will be marked with a suspect flag:

- There is loss of continuity (LOC) during a measurement interval. If the LOC alarm is raised in the maintenance entity group end point (MEP) by continuity check messages (CCMs) during a measurement interval, the suspect flag will be raised for that measurement interval.
- The clock is adjusted by more than 10 seconds. If the system clock is adjusted by more than 10 seconds during a measurement interval, the suspect flag will be raised.
- The performance monitoring session is started during a measurement interval. If the session starts during a measurement interval (for example, a performance monitoring session is initiated at 3:00 with a measurement interval of 5 minutes, and the start time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The performance session is stopped during a measurement interval. If the session stops during a measurement interval (for example, a performance monitoring session was initiated at 3:00 with a measurement interval of 5 minutes, and the stop time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The Ethernet virtual circuit (EVC) status transitions to **Not Running** during a measurement interval. If the EVC over which the performance monitoring session is conducted transitions to a **Not Running** state during a measurement interval, the suspect flag will be raised for that measurement interval.
- The MEP transitions to an **Unavailable** or **Out of Service** state during a measurement interval. If the MEP goes to an **Unavailable** or **Out of Service** state during a measurement interval, the suspect flag will be raised for that measurement interval.

Usage Examples

The following example specifies that averaged ETH-DM measurement interval data should be saved to the performance monitoring logs:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#frame-delay two-way file-save averaged**

frame-loss single-ended

Use the **frame-loss single-ended** command to monitor frame loss across maintenance entity group (MEG) endpoints (MEPs) by counting in-profile customer frames. Use the **no** form of this command to disable the monitoring feature. Variations of this command include:

frame-loss single-ended <*mep id*> **priority** <*value*>
frame-loss single-ended <*target mac address*> **priority** <*value*>
frame-loss single-ended multicast priority <*value*>

Syntax Description

<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191**.
<*target mac address*>	Specifies the medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
priority <*value*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.

Default Values

By default, no frame loss monitoring sessions are configured.

Command History

Release R11.6.0	Command was introduced.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a frame loss monitoring session for MEP **100** with a priority of **3**:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#frame-loss single-ended 100 priority 3**

frame-loss single-ended file-save averaged

Use the **frame-loss single-ended file-save averaged** command to specify that averaged single-ended frame loss (ETH-LM) measurement interval data is saved to performance monitoring logs. Use the **no** form of this command to disable saving data to the performance monitoring logs.

Syntax Description

No subcommands.

Default Values

By default, the ETH-LM measurement interval data is not saved to the performance monitoring logs.

Command History

Release 11.6.0	Command was introduced.

Functional Notes

By default, each time a new measurement interval occurs during a Y.1731 performance monitoring session, ETH-DM, ETH-LM, and ETH-SLM, the data from the previous interval is overwritten. The performance monitoring file save feature allows performance monitoring logs to be stored in memory in a series of hour-long log files. The unit records session data to the current log file at user-specified intervals. At the end of the user-specified log lifetime, the logs are rotated out in a first-in first-out fashion; the oldest files are deleted to make room for the new files. Each performance monitoring session type is stored in a separate file in the user-specified directory. The file is automatically named by the unit using the following format:

<*device serial*>**_<DM | LM | SLM>.Data_**<*date and time*>**.pm.xz[.current]**

Parameter	Description
<*device serial*>	Specifies the serial number of the unit.
DM	Specifies that the file is a single-ended (two-way) frame delay log.
LM	Specifies that the file is a single-ended frame loss log.
SLM	Specifies that the file is a single-ended synthetic frame loss log.
<*date and time*>	Specifes the date and time at which the log ends in the format **YYYY-MM-DD_hh.mm.ss**, for example: **2014-12-30_14:00:00**. This specifies the last time interval that the file will be written.
.pm.xz	Specifies the file extension of the log file.
.current	Appended to files that are still in use and could have data written to them.

The following example is a sample ETH-SLM file name that is no longer writable:

LBADTN340767_SLM.Data_2014-12-04_15.00.00.pm.xz

The following example is a sample ETH-LM file name of a file to which the unit is currently writing:

LBADTN340767_LM.Data_2014-12-04_15.00.00.pm.xz.current

If the file directory for the log files is changed, the files in the previous save directory will not be deleted for log rotation. Log rotation only occurs for files in the currently-specified save directory.

If any of the following conditions occur during a measurement interval, the measurement will be considered suspect, and it will be marked with a suspect flag:

- There is loss of continuity (LOC) during a measurement interval. If the LOC alarm is raised in the maintenance entity group end point (MEP) by continuity check messages (CCMs) during a measurement interval, the suspect flag will be raised for that measurement interval.
- The clock is adjusted by more than 10 seconds. If the system clock is adjusted by more than 10 seconds during a measurement interval, the suspect flag will be raised.
- The performance monitoring session is started during a measurement interval. If the session starts during a measurement interval (for example, a performance monitoring session is initiated at 3:00 with a measurement interval of 5 minutes, and the start time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The performance session is stopped during a measurement interval. If the session stops during a measurement interval (for example, a performance monitoring session was initiated at 3:00 with a measurement interval of 5 minutes, and the stop time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The Ethernet virtual circuit (EVC) status transitions to **Not Running** during a measurement interval. If the EVC over which the performance monitoring session is conducted transitions to a **Not Running** state during a measurement interval, the suspect flag will be raised for that measurement interval.
- The MEP transitions to an **Unavailable** or **Out of Service** state during a measurement interval. If the MEP goes to an **Unavailable** or **Out of Service** state during a measurement interval, the suspect flag will be raised for that measurement interval.

Usage Examples

The following example specifies that averaged ETH-LM measurement interval data should be saved to the performance monitoring logs:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#frame-loss single-ended file-save averaged**

frame-loss synthetic single-ended

Use the **frame-loss synthetic single-ended** command to monitor frame loss across maintenance entity group (MEG) endpoints (MEPs) by counting synthetic data frames. Use the **no** form of this command to disable the monitoring feature. Variations of this command include:

frame-loss synthetic single-ended <*mep id*> **priority** <*value*>
frame-loss synthetic single-ended <*target mac address*> **priority** <*value*>
frame-loss synthetic single-ended multicast priority <*value*>

Syntax Description

<*mep id*>	Specifies the MEP ID of the target MEP. Valid MEP ID range is **1** to **8191**.
<*target mac address*>	Specifies the medium access control (MAC) address of the target MEP. Enter MAC addresses in hexadecimal format, for example: **xx:xx:xx:xx:xx:xx**.
multicast	Specifies the session is configured for multicast.
priority <*value*>	Optional. Specifies the virtual local area network (VLAN) priority of the target MEP. Valid range is **0** to **7**.

Default Values

By default, no frame loss monitoring sessions are configured.

Command History

Release R10.10.0	Command was introduced.
Release R11.10.0	Command was expanded to include the **multicast** parameter.

Usage Examples

The following example configures a frame loss monitoring session for MEP **100** with a priority of **3**:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#frame-loss synthetic single-ended 100 priority 3**

frame-loss synthetic single-ended file-save averaged

Use the **frame-loss synthetic single-ended file-save averaged** command to specify that averaged single-ended synthetic frame loss (ETH-SLM) measurement interval data is saved to performance monitoring logs. Use the **no** form of this command to disable saving data to the performance monitoring logs.

Syntax Description

No subcommands.

Default Values

By default, the ETH-SLM measurement interval data is not saved to the performance monitoring logs.

Command History

Release 11.6.0	Command was introduced.

Functional Notes

By default, each time a new measurement interval occurs during a Y.1731 performance monitoring session, ETH-DM, ETH-LM, and ETH-SLM, the data from the previous interval is overwritten. The performance monitoring file save feature allows performance monitoring logs to be stored in memory in a series of hour-long log files. The unit records session data to the current log file at user-specified intervals. At the end of the user-specified log lifetime, the logs are rotated out in a first-in first-out fashion; the oldest files are deleted to make room for the new files. Each performance monitoring session type is stored in a separate file in the user-specified directory. The file is automatically named by the unit using the following format:

*<device serial>***_<DM | LM | SLM>.Data_***<date and time>***.pm.xz[.current]**

Parameter	Description
<device serial>	Specifies the serial number of the unit.
DM	Specifies that the file is a single-ended (two-way) frame delay log.
LM	Specifies that the file is a single-ended frame loss log.
SLM	Specifies that the file is a single-ended synthetic frame loss log.
<date and time>	Specifes the date and time at which the log ends in the format **YYYY-MM-DD_hh.mm.ss**, for example: **2014-12-30_14:00:00**. This specifies the last time interval that the file will be written.
.pm.xz	Specifies the file extension of the log file.
.current	Appended to files that are still in use and could have data written to them.

The following example is a sample ETH-SLM file name that is no longer writable:

LBADTN340767_SLM.Data_2014-12-04_15.00.00.pm.xz

The following example is a sample ETH-LM file name of a file to which the unit is currently writing:

LBADTN340767_LM.Data_2014-12-04_15.00.00.pm.xz.current

> NOTE *If the file directory for the log files is changed, the files in the previous save directory will not be deleted for log rotation. Log rotation only occurs for files in the currently-specified save directory.*

If any of the following conditions occur during a measurement interval, the measurement will be considered suspect, and it will be marked with a suspect flag:

- There is loss of continuity (LOC) during a measurement interval. If the LOC alarm is raised in the maintenance entity group end point (MEP) by continuity check messages (CCMs) during a measurement interval, the suspect flag will be raised for that measurement interval.
- The clock is adjusted by more than 10 seconds. If the system clock is adjusted by more than 10 seconds during a measurement interval, the suspect flag will be raised.
- The performance monitoring session is started during a measurement interval. If the session starts during a measurement interval (for example, a performance monitoring session is initiated at 3:00 with a measurement interval of 5 minutes, and the start time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The performance session is stopped during a measurement interval. If the session stops during a measurement interval (for example, a performance monitoring session was initiated at 3:00 with a measurement interval of 5 minutes, and the stop time is set to 3 minutes after 3:00) then the suspect flag will be raised for that measurement interval.
- The Ethernet virtual circuit (EVC) status transitions to **Not Running** during a measurement interval. If the EVC over which the performance monitoring session is conducted transitions to a **Not Running** state during a measurement interval, the suspect flag will be raised for that measurement interval.
- The MEP transitions to an **Unavailable** or **Out of Service** state during a measurement interval. If the MEP goes to an **Unavailable** or **Out of Service** state during a measurement interval, the suspect flag will be raised for that measurement interval.

Usage Examples

The following example specifies that averaged ETH-SLM measurement interval data should be saved to the performance monitoring logs:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#frame-loss synthetic single-ended file-save averaged**

priority *<value>*

Use the **priority** command to specify the priority given to connectivity fault management (CFM) frames and linktrace messages transmitted by the maintenance entity group end point (MEP). Use the **no** form of this command to return the priority to the default value.

Syntax Description

<value>	Specifies the priority. Range is **0** to **7**.

Default Values

By default, the priority value is **7**.

Command History

Release 17.4	Command was introduced.
Release R10.10.0	Command was expanded to include the Y.1731 local MEP.

Usage Examples

The following example specifies a priority of **3** for CFM frames and linktrace messages transmitted by this MEP:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#priority 3**

set interface

Use the **set interface** command to associate an interface or Ethernet in the first mile (EFM) group with the maintenance entity group end point (MEP). Use the no form of this command to remove the specified association. Variations of this command include:

set interface efm-group <*slot/group*>
set interface gigabit-ethernet <*slot/port*>

Syntax Description

efm-group <*slot/group*>	Associates the specified EFM group with the MEP.
gigabit-ethernet <*slot/port*>	Associates the specified Gigabit Ethernet interface with the MEP.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example associates Gigabit Ethernet interface **1/1** with the MEP:

(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)**#set interface gigabit-ethernet 1/1**

Y.1731 MEG COMMAND SET

A maintenance entity group (MEG) object, as defined by Y.1731, includes different maintenance entities (MEs) that satisfy the following conditions: MEs in a MEG exist in the same administrative boundary, MEs in a MEG have the same MEG level, and MEs in a MEG belong to the same point-to-point or multipoint Ethernet connection. A MEG is a collection of MEs, and an ME refers to the direct connection between two MEG end points (MEPs) in a MEG. A MEP forms an ME with every other MEP in the same MEG. The MEG's MEG level attribute is used by all MEPs created within it.

The minimum attributes required to create or access a MEG are the MEG ID and MEG level after which the MEG attributes can be edited to make ready for operation. The reason why both MEG ID and MEG Level must be used to create the MEG is to allow MEGs with the same name but different MEG levels to be unique. This may be required if the administrator needs to interoperate with devices not under their control which use the same MEG ID but operate at different MEG Levels.

MEG groups are created and configured using the **ethernet y1731 meg** command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#ethernet y1731 meg char-string MEG1 level 1
(config-y1731-meg MEG1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

ccm interval

Use the **ccm interval** command to specify the interval at which the local maintenance entity group end point (MEP) will transmit continuity check messages (CCMs) and the interval at which it expects to receive CCMs from each peer in the MEG. Use the **no** form of this command to return the CCM interval to the default value. Variations of this command include:

ccm interval 1-minute
ccm interval 1-second
ccm interval 10-minutes
ccm interval 10-seconds
ccm interval 100-milliseconds

Syntax Description

1-minute	Specifies a 1 minute CCM interval.
1-second	Specifies a 1 second CCM interval.
10-minutes	Specifes a 10 minute CCM interval.
10-seconds	Specifies a 10 second CCM interval.
100-milliseconds	Specifies a 100 millisecond CCM interval.

Default Values

By default, the CCM interval is 1 minute.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example configures the MEG with a CCM interval of 1 second:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#ccm interval 1-second**

local-mep *<id>*

Use the **local-mep** command to create a maintentance entity group end point (MEP) and access the Local MEP Configuration mode. Use the **no** form of this command to remove the MEP.

Syntax Description

<id>	Specifies the MEP identifier (ID) of the local MEP. Valid range is **1** to **8191**.

Default Values

By default, no MEPs are configured.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example creates a local MEP with a MEP ID of **3** on **MEG1**:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#local-mep 3**
MEP 3 created
(config-y1731-mep3)#

mep database clear

Use the **mep database clear** command to clear the discovered remote maintentance entity group end point (MEP) from the MEP database. Variations of this command include:

mep database clear
mep database clear *<id>*

Syntax Description

<id>	Specifies the remote MEP (RMEP) identifier (ID) to remove from the MEP database. Valid range is **1** to **8191**.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example clears all discovered RMEPs from the MEP database:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#mep database clear**

mep database lock

Use the **mep database lock** command to lock the discovered remote maintentance entity group end point (MEP) into the MEP database. Variations of this command include:

mep database lock
mep database lock <*id*>

Syntax Description

<*id*>	Specifies the remote MEP (RMEP) identifier (ID) to lock into the MEP database. Valid range is **1** to **8191**.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example locks all discovered RMEPs into the MEP database:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#mep database lock**

mep database rule

Use the **mep database rule** command to configure the rules for adding new entries into the remote maintentance entity group end point (MEP) database. Variations of this command include:

mep database rule auto-discovery
mep database rule auto-learning
mep database rule configured-only

Syntax Description

auto-discovery	Specifies that when continuity check messages (CCMs) are received from remote MEPs (RMEPs), they are added as discovered RMEPs in the MEP database.
auto-learning	Specifies that when continuity check messages (CCMs) are received from remote MEPs (RMEPs), they are added as static RMEPs in the MEP database.
configured-only	Specifies that CCMs must match the configured static RMEP entries.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example allows new RMEPs to be added as discovered RMEPs in the MEP database:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#mep database rule auto-discovery**

remote-mep *<id>*

Use the **remote mep** command to add a maintentance entity group end point (MEP) to the list of expected continuity check message (CCM) sources. Use the no form of this command to remove a MEP from the list.

Syntax Description

<id>	Specifies the remote MEP (RMEP) identifier (ID) to add to the list of expected CCM sources. Valid range is **1** to **8191**.

Default Values

By default, no RMEPs are configured as CCM sources.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example configures RMEP **25** as an expected CCM source:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#remote-mep 25**

service

Use the **service** command to specify the service type and service value of traffic on the maintenance entity group (MEG). Variations of this command include:

service single-tagged ce-vlan-id <*tag*>
service single-tagged s-tag <*tag*>
service double-tagged s-tag <*tag*> **ce-vlan-id** <*tag*>

Syntax Description

single-tagged	Specifies that the L2 header of the Y.1731 packets to be processed should contain either a customer edge virtual local area network (CE-VLAN) identifier (ID) tag or a service tag (s-tag) with the specified value.
double-tagged	Specifies that the L2 header of the Y.1731 packets to be processed should contain both a CE-VLAN ID tag and an s-tag with the specified values.
ce-vlan-id <*vlan tag*>	Specifies the CE-VLAN ID of traffic on the MEG. Valid range is **1** to **4094**.
s-tag <*s-tag*>	Specifies the s-tag of traffic on the MEG. Valid range is **1** to **4094**.

Default Values

No default values are necessary for this command.

Command History

Release R10.10.0	Command was introduced.
Release R11.5.0	The **double-tagged** parameter was added.

Functional Notes

This feature is used together with the Y.1731 EtherType, level, and local and remote maintenance entity group end point (MEP) ID to identify Y.1731 packets that should be processed by the maintenance point (MP).

Usage Examples

The following example specifies that packets should contain an **s-tag** with a value of **54**:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#service single-tagged s-tag 54**

The following example specifies that packets should contain an **s-tag** with a value of **54** and a CE-VLAN ID of **12**:

(config)**#ethernet y1731 meg char-string MEG1 level 1**
(config-y1731-meg MEG1)**#service double-tagged s-tag 54 ce-vlan-id 12**

ROUTING PROTOCOL COMMAND SETS

The routing protocol command sets are divided into the following sections:

BGP COMMAND SETS

This section includes the following command sets:

AS PATH LIST COMMAND SET

To activate the Autonomous System (AS) Path List Configuration mode, enter the **ip as-path-list** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip as-path-list MyList
(config-as-path-list)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

deny <value> on page 3979
permit <value> on page 3980

deny *<value>*

Use the **deny** command to add an entry to the community list that denies Border Gateway Protocol (BGP) routes containing the specified community number in the community attribute. Use the **no** form of this command to remove the statement from the community list.

Syntax Description

<value>	Denies routes that contain this value in their community attribute. This is a numeric value that can be an integer from **1** to **4294967295** or string in the form ***aa:nn***, where ***aa*** is the autonomous system (AS) number and ***nn*** is the community number. Multiple community number parameters can be present in the command.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates a community list named **MyList** to deny BGP routes that match the AS path attributes **30:22**:

(config)**#ip as-path-list MyList**
(config-as-path-list)**#deny 30:22**

permit <*value*>

Use the **permit** command to add an entry to the community list that allows only Border Gateway Protocol (BGP) routes containing the specified community number in the community attribute. Use the **no** form of this command to remove the statement from the community list.

Syntax Description

<*value*>	Permits routes that contain this value in their community attribute. This is a numeric value that can be an integer from **1** to **4294967295** or string in the form ***aa:nn***, where ***aa*** is the autonomous system (AS) number and ***nn*** is the community number. Multiple community number parameters can be present in the command.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates a community list named **MyList** to permit BGP routes that match the AS path attributes **30:22**:

(config)**#ip as-path-list MyList**
(config-as-path-list)**#permit 30:22**

BGP COMMAND SET

BGP is an Exterior Gateway Protocol (EGP) that is used within the Internet and multinational organizations. EGP is one of two different types of dynamic routing protocols. The other protocol is Interior Gateway Protocol (IGP). The difference between the two protocols is that IGPs (for example, Routing Information Protocol (RIP), Open Shortest Path First (OSPF)) operate within an autonomous system (AS), whereas EGPs allow routes to be exchanged between different autonomous systems. Typically, an AS is defined by the boundaries of an organization. As an EGP, BGP routes must regulate traffic between networks controlled by organizations with different policies. BGP is designed to allow administrators to customize a policy for route exchange. The following are some characteristics of BGP that make it an appropriate protocol for connecting different autonomous systems:

- BGP can filter both the routes it receives and those that it sends according to bit length, thereby minimizing the number of routes exchanged.
- BGP uses policies to determine best routes rather than per-hop counts used in RIP or link states used in OSPF. Each AS can set their own policy.
- BGP routers communicate only with manually configured neighbors.
- You can configure different policies for route exchange with different neighbors.
- Multiple virtual routing and forwarding (Multi-VRF) BGP allows each VRF instance from the service provider its own BGP session within the router, thus extending the VRF instance from the service provider to the router.

In AOS firmware release 18.03.00, Multi-VRF BGP functionality was incorporated into AOS. This release allows BGP configuration to occur on different VRF instances, and changes the hierarchical structure of BGP within AOS, as well as the configuration steps necessary for BGP configuration. In addition, in AOS firmware release R10.1.0, support for multiprotocol BGP and Internet Protocol version 6 (IPv6) BGP were added.

The following are new features of BGP included with Multi-VRF BGP.

Address families (AFs) are used in BGP to maintain a separation between Internet protocol types within a VRF instance. With the advent of Multi-VRF BGP in 18.03.00, AOS implemented the use of AFs into the BGP hierarchical structure. An AF is a configuration structure that can reside at the default VRF instance and within a nondefault VRF instance. Creating an address family enables processing of that address family within a VRF, and it provides a place for AF-specific configuration.

In addition to the use of AFs, Multi-VRF BGP also allows the recognition and configuration of VRF instances specific to BGP functionality within the router. This allows the VRF constructs from the service provider to be incorporated into the customer router.

Multi-VRF is an application of the typical BGP functionality. As the name suggests, Multi-VRF BGP extends traditional service provider multi-VRF functionality of BGP to the customer edge router. This type of feature is typically used in Layer 3 virtual private network (VPN) applications where the VPN is extended to the customer device using Multi-VRF. Multi-VRF BGP allows the customer edge router to dynamically exchange customer VPN routers to and through the provider's VPN *cloud*, thus eliminating the reliance on the provider to manage static routes. Multi-VRF takes place on the link between the service provider's routers and the customer edge equipment.

In Multi-VRF BGP the concepts of the address family and VRF instances are incorporated into the BGP configuration structure. VRF instances are in themselves not tied to a specific protocol, and therefore, control of multiple protocols within a single VRF is accomplished using an AF. Multi-VRF BGP also uses the concepts of AFs to provide specific BGP configuration to a single BGP policy, and maintain control over multiple BGP policies within a single AF.

In Multi-VRF BGP, the hierarchical structure of BGP configuration is as follows:

```
Global BGP settings (affecting all of BGP for this router)
!
VRF BGP settings (affecting only the default VRF)
Neighbor #1 Definition
    Neighbor #1 common settings (common to all peering with neighbor #1)
    exit
!
Address Family for the default VRF
    AF BGP settings (affecting only this AF)
    Neighbor #1 Reference
        Neighbor #1 AF-specific settings
        exit
    exit
!
VRF name1
    VRF BGP settings (affecting only this vRF)
    Neighbor #2 Definition
        Neighbor #2 common settings (common to all peering with neighbor #2)
        exit
!
Address Family for VRF name1
    AF BGP settings (affecting this AF)
    Neighbor #2 Reference
        Neighbor #2 settings specific to this AF
        exit
    exit
exit
```

Because the structure of BGP changed with the AOS 18.03.00 release, there are several sections of BGP configuration commands. The following are the BGP configuration command sections for AOS products, and are applicable to both the default and nondefault VRF instances:

- *BGP Command Set on page 3981*
- *BGP Address Family Command Set on page 4001*
- *BGP AF Neighbor Command Set on page 4022*
- *BGP Neighbor Command Set on page 4041*

To enable BGP in AOS products, and activate the BGP Configuration mode, enter the **router bgp** command at the Global Configuration mode prompt followed by the AS number of the local system of which this BGP router is a member. To enter the BGP Configuration mode for the default VRF, enter the command as follows:

```
>enable
#configure terminal
(config)#router bgp 100
(config-bgp)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

address-family on page 3984
bgp on page 3986
bgp default local-preference <value> on page 3988
bgp fast-external-failover on page 3990
bgp log-neighbor-changes on page 3992
bgp router-id <ipv4 address> on page 3994
hold-timer <value> on page 3996
neighbor on page 3998
vrf <name> on page 4000

address-family

Use the **address-family** command to configure the Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) address family (AF) for the default or nondefault virtual routing and forwarding (VRF) instances on the AOS device. This command also enters the AF's configuration mode. Use the **no** version of this command to remove the AF from the BGP configuration. Variations of this command include:

address-family ipv4
address-family ipv6

Syntax Description

ipv4	Creates an IPv4 BGP AF.
ipv6	Creates an IPv6 BGP AF.

Default Values

By default, the AF is not configured on either the default or nondefault VRF instance.

Command History

Release 18.3	Command was introduced.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **address-family** command can be used to create an AF on either the default or nondefault VRF instance. If the AF is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#**

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates an IPv4 AF on the default VRF instance and enters the AF's configuration mode:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)#

The following example creates an IPv4 AF on the nondefault VRF instance named **RED1** and enters the AF's configuration mode:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

bgp

Use the **bgp** command to instruct AOS on how to handle multi-exit discriminators (MEDs) for all Border Gateway Protocol (BGP) routes from the same autonomous system (AS) on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to disable this feature. Variations of this command include:

bgp always-compare-med
bgp compare-med
bgp deterministic-med
bgp ignore-med

Syntax Description

always-compare-med	Configures AOS to always compare MEDs for all paths for a route, regardless of the AS through which the paths pass.
compare-med	Configures AOS to compare MEDs for all received routes.
deterministic-med	Configures AOS to compare the MEDs for all routes received from different neighbors within the same AS.
ignore-med	Configures AOS to disregard MEDs for all received routes.

Default Values

By default, AOS compares the MED attributes for routes from the same AS.

Command History

Release 11.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **bgp** command can be used to specify MED behavior on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables MED options on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#bgp compare-med**

The following example enables MED options on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#bgp compare-med**

bgp default local-preference <*value*>

Use the **bgp default local-preference** command to change the local preference for all Border Gateway Protocol (BGP) routes on either the default or nondefault virtual routing and forwarding (VRF) instances. The local preference is an attribute (LOCAL_PREF) that indicates a degree of preference for a route relative to other routes in the local autonomous system (AS). BGP neighbors can send the local preference value as an attribute of a route in an UPDATE message. Local preference only applies to routes within the local AS. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the local preference value. Valid range is **0** to **4294967295**.

Default Values

By default, the local preference is set to **100**.

Command History

Release 11.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **bgp default local-preference** command can be used to specify the local preference on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example changes the default local preference to **200** for the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#bgp default local-preference 200**

The following example changes the default local preference to **200** for the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#bgp default local-preference 200**

bgp fast-external-failover

Use the **bgp fast-external-failover** command to enable the fast-external-failover feature for Border Gateway Protocol (BGP) on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **bgp fast-external-failover** command can be used to enable fast-external-failover on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

When enabled, if the link interface over which the router is communicating with a BGP peer goes down, the BGP session with that peer is immediately cleared. When failover is disabled and the link goes down, the session is maintained until the BGP hold timer expires.

Usage Examples

The following example enables fast-external-failover on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#bgp fast-external-failover**

The following example enables fast-external-failover on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#bgp fast-external-failover**

bgp log-neighbor-changes

Use the **bgp log-neighbor-changes** command to control the logging of Border Gateway Protocol (BGP) neighbor state changes on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, BGP neighbor changes are not logged.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **bgp log-neighbor-changes** command can be used to log BGP neighbor activity on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

This command controls logging of BGP neighbor state changes (up/down) and resets. This information is useful for troubleshooting and determining network stability.

Usage Examples

The following example enables logging of BGP neighbor state changes on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#bgp log-neighbor-changes**

The following example enables logging of BGP neighbor state changes on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#bgp log-neighbor-changes**

bgp router-id *<ipv4 address>*

Use the **bgp router-id** command to specify the Internet Protocol version 4 (IPv4) address that the router should use as its Border Gateway Protocol (BGP) router ID. This command can be applied to either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

<ipv4 address>	Designates the IPv4 address this router should use as its BGP router ID. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no router ID is configured. The default action is detailed in *Functional Notes* below.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **bgp router-id** command can be used to specify the IPv4 address used for the router ID on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

The **bgp router-id** command allows an IPv4 address to be specified for use as the BGP router ID. If no IPv4 address is configured at BGP startup, it uses the highest IPv4 address configured on a loopback interface. If no loopback interfaces are configured, it uses the highest IPv4 address configured on any interface that is active. If the specified router ID is changed, existing sessions with BGP neighbors are reset.

Usage Examples

The following example configures IPv4 address **10.0.0.1** as the BGP router ID on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#bgp router-id 10.0.0.1**

The following example configures IPv4 address **10.0.0.1** as the BGP router ID on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#bgp router-id 10.0.0.1**

hold-timer <*value*>

Use the **hold-timer** command to set the default hold time for all neighbors in the Border Gateway Protocol (BGP) process on either the default or nondefault virtual routing and forwarding (VRF) instance.

Syntax Description

<*value*>	Specifies a time interval (in seconds) within which a keepalive must be received from a peer before that peer is declared dead. Range is **0** to **65535** seconds.

Default Values

By default, the hold time is **180** seconds.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **hold-timer** command can be used to specify the hold timer for BGP neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have configured the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Using the **hold-timer** command in BGP configuration mode sets the default hold time for all neighbors in that BGP process. Using the **hold-timer** command in BGP Neighbor Configuration mode sets the hold time for only that neighbor. The peers will negotiate and use the lowest configured setting. The keepalive interval will be set to one-third of the negotiated hold time.

Usage Examples

The following example sets a hold time of **120** seconds for a specific neighbor, with an understood keepalive interval of **40** seconds on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#hold-timer 120**

The following example sets a hold time of **120** seconds for a specific neighbor, with an understood keepalive interval of **40** seconds on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#hold-timer 120**

neighbor

Use the **neighbor** command to create a Border Gateway Protocol (BGP) neighbor, specify an Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) address, and enter the BGP Neighbor configuration mode. Refer to *BGP Neighbor Command Set on page 4041* for more information on neighbor-specific configuration parameters. This command can be used for either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the configured neighbors. Variations of this command include:

neighbor <*ipv4 address*>
neighbor <*ipv4 address*> **mef-ethernet** <*slot/port*>
neighbor <*ipv4 address*> **system-control-evc**
neighbor <*ipv4 address*> **system-management-evc**
neighbor <*ipv6 address*>
neighbor <*ipv6 address*> **mef-ethernet** <*slot/port*>
neighbor <*ipv6 address*> **system-control-evc**
neighbor <*ipv6 address*> **system-management-evc**

Syntax Description

<*ipv4 address*>	Specifies the IPv4 address for the neighbor. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*ipv6 address*>	Specifies the IPv6 address for the neighbor. IPv6 addresses should be expressed in dotted decimal notation (for example, **2001:DB8:1::1**).
mef-ethernet <*slot/port*>	Optional. Specifies the neighbor is the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the neighbor is a member of the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Specifies the neighbor is a member of the system management EVC.

Default Values

By default, there are no configured BGP neighbors.

Command History

Release 11.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

The **neighbor** command can be used to specify the BGP neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures an IPv4 BGP neighbor with an IPv4 address of **10.10.10.1** on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#neighbor 10.10.10.1**
(config-bgp-neighbor)#

The following example configures an IPv4 BGP neighbor with an IPv4 address of **10.10.10.1** on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.10.10.1**

The following example configures an IPv4 BGP neighbor with an address of **10.10.10.1** on the nondefault VRF instance named **RED1** and specifies this neighbor is a member of the system control EVC:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.10.10.1 system-control-evc**

vrf *<name>*

Use the **vrf** command to associate a specific virtual routing and forwarding (VRF) instance with Border Gateway Protocol (BGP) configurations and enter the BGP Configuration mode on the nondefault VRF instance. This command allows you to configure the BGP settings for the specified VRF instance. Use the **no** form of this command to remove the association between the named VRF instance and the BGP configuration.

Syntax Description

<name>	Specifies the name of the VRF instance to associate with BGP.

Default Values

By default, BGP configurations are associated with the default (unnamed) VRF instance.

Command History

Release 17.1	Command was introduced.
Release 18.3	Command was added to BGP and Dynamic Host Control Protocol (DHCP) version 4 (DHCPv4) and version 6 (DHCPv6).
Release R11.2.0	Command was added to network monitoring

Functional Notes

VRF instances must be created first before they can be assigned to BGP configuration. Create the VRF instance using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the VRF instance named **RED1** and enters the BGP configuration mode for the nondefault VRF:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)#

BGP ADDRESS FAMILY COMMAND SET

In AOS firmware release 18.03.00, Multiple virtual routing and forwarding (VRF) Border Gateway Protocol (BGP) functionality was incorporated into AOS. This release allows BGP configuration to occur on different VRF instances, and changes the hierarchical structure of BGP within AOS as well as the configuration steps necessary for BGP configuration. In addition, in AOS firmware release R10.1.0, multiprotocol BGP and BGP for Internet Protocol version 6 (IPv6) were added.

The following are new features of BGP included with Multi-VRF BGP, multiprotocol BGP, and BGP for IPv6.

Address families (AFs) are used in BGP to maintain a separation between Internet protocol types within a VRF instance. With the advent of Multi-VRF BGP in 18.03.00, AOS implemented the use of AFs into the BGP hierarchical structure. An AF is a configuration structure that can reside at the default VRF instance and within a nondefault VRF instance. Creating an address family enables processing of that address family within a VRF, and it provides a place for AF-specific configuration.

In addition to the use of AFs, Multi-VRF BGP also allows the recognition and configuration of VRF instances specific to BGP functionality within the router. This allows the VRF constructs from the service provider to be incorporated into the customer router.

Multi-VRF is an application of the typical BGP functionality. As the name suggests, Multi-VRF BGP extends traditional service provider multi-VRF functionality of BGP to the customer edge router. This type of feature is typically used in Layer 3 virtual private network (VPN) applications where the VPN is extended to the customer device using multi-VRF. Multi-VRF BGP allows the customer edge router to dynamically exchange customer VPN routers to and through the provider's VPN *cloud*, thus eliminating the reliance on the provider to manage static routes. Multi-VRF takes place on the link between the service provider's routers and the customer edge equipment.

In Multi-VRF BGP the concepts of the address family and VRF instances are incorporated into the BGP configuration structure. VRF instances are in themselves not tied to a specific protocol, and therefore, control of multiple protocols within a single VRF is accomplished using an AF. Multi-VRF BGP also uses the concepts of AFs to provide specific BGP configuration to a single BGP policy, and maintain control over multiple BGP policies within a single AF.

In Multi-VRF BGP, the hierarchical structure of BGP configuration is as follows:

```
Global BGP settings (affecting all of BGP for this router)
!
VRF BGP settings (affecting only the default VRF)
Neighbor #1 Definition
    Neighbor #1 common settings (common to all peering with neighbor #1)
    exit
!
Address Family for the default VRF
    AF BGP settings (affecting only this AF)
    Neighbor #1 Reference
```



```
        Neighbor #1 AF-specific settings
        exit
    exit
!
VRF name1
    VRF BGP settings (affecting only this vRF)
    Neighbor #2 Definition
        Neighbor #2 common settings (common to all peering with neighbor #2)
        exit
!
Address Family for VRF name1
    AF BGP settings (affecting this AF)
    Neighbor #2 Reference
        Neighbor #2 settings specific to this AF
        exit
    exit
exit
```

Because the structure of BGP changed with the AOS 18.03.00 release, there are several sections of BGP configuration commands. The following are the BGP configuration command sections for AOS products, and are applicable to both the default and nondefault VRF instances:

- *BGP Command Set on page 3981*
- *BGP Address Family Command Set on page 4001*
- *BGP AF Neighbor Command Set on page 4022*
- *BGP Neighbor Command Set on page 4041*

Once you have enabled BGP in AOS products, you can enter the AF Configuration mode by entering the **address-family** command at the BGP Configuration mode prompt. To enter the IPv4 BGP AF Configuration mode for the default VRF, enter the command as follows:

```
>enable
#configure terminal
(config)#router bgp 100
(config-bgp)#address-family ipv4
(config-bgp-ipv4)#
```

To enter the IPv6 BGP AF Configuration mode for the default VRF, enter the command as follows:

```
>enable
#configure terminal
(config)#router bgp 100
(config-bgp)#address-family ipv6
(config-bgp-ipv6)#
```


The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

distance bgp <external> <internal> <local> on page 4004
maximum-paths <value> on page 4006
neighbor on page 4008
network <ipv4 address> mask <subnet mask> on page 4010
network <ipv6 address/prefix-length> on page 4012
redistribute connected on page 4014
redistribute ospf on page 4016
redistribute rip on page 4018
redistribute static on page 4020

distance bgp *<external> <internal> <local>*

Use the **distance bgp** command to set the administrative distance for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) address family (AF) routes on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting. Variations of this command include:

distance bgp *<external>*
distance bgp *<external> <internal>*
distance bgp *<external> <internal> <local>*

Syntax Description

<external>	Sets the administrative distance for BGP routes learned via external Border Gateway Protocol (eBGP) sessions. Range is **1** to **255**.
<internal>	Optional. Sets the administrative distance for BGP routes learned via internal Border Gateway Protocol (iBGP) sessions. Range is **1** to **255**.
<local>	Optional. Sets the administrative distance for BGP routes learned via the network command and redistribution. Range is **1** to **255**.

Default Values

By default, external is set to **20**, internal to **200**, and local to **200**. Normally, these default settings should not be changed.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **distance** command can be used to allow a BGP AF on either the default or nondefault VRF instance to select the best route when there are multiple routes to the same network. If the AF is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

This command sets the administrative distance for BGP routes. The administrative distance is a local variable that allows a router to choose the best route when there are multiple paths to the same network. Routes with lower administrative distances are preferable.

Usage Examples

The following example gives external BGP routes an administrative distance of **30**, internal BGP routes an administrative distance of **200**, and local routes an administrative distance of **240** for the IPv4 BGP AF on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#distance bgp 30 200 240**

The following example gives external BGP routes an administrative distance of **30**, internal BGP routes an administrative distance of **200**, and local routes an administrative distance of **240** for the IPv4 BGP AF on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#distance bgp 30 200 240**

maximum-paths *<value>*

Use the **maximum-paths** command to specify the number of equal cost parallel routes (shared paths) learned by the Border Gateway Protocol (BGP) address family (AF) that can be exported to the route table. When IP load sharing is enabled, traffic is balanced to a specific destination across up to six equal paths. This command can be used for a BGP AF on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the number of equal cost parallel routes learned by BGP AFs that can be exported to the route table. Valid range is **1** to **6**.

Default Values

By default, a single path can exist in the route table.

Command History

Release 11.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **maximum-paths** command can be used to specify the number of paths for a BGP AF on either the default or nondefault VRF instance to select the best route when there are multiple routes to the same network. If the AF is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures the IPv4 BGP AF on the default VRF instance to export **4** parallel paths to the route table:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#maximum-paths 4**

The following example configures the IPv4 BGP AF on the nondefault VRF instance named **RED1** to export **4** parallel paths to the route table:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#maximum-paths 4**

neighbor

Use the **neighbor** command to create a Border Gateway Protocol (BGP) address family (AF) neighbor, specify an Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) address, and enter the BGP AF Neighbor Configuration mode. Refer to *BGP AF Neighbor Command Set on page 4022* for more information on AF neighbor-specific configuration parameters. This command can be used for either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the configured neighbors. Variations of this command include:

neighbor <*ipv4 address*>
neighbor <*ipv4 address*> **mef-ethernet** <*slot/port*>
neighbor <*ipv4 address*> **system-control-evc**
neighbor <*ipv4 address*> **system-management-evc**
neighbor <*ipv6 address*>
neighbor <*ipv6 address*> **mef-ethernet** <*slot/port*>
neighbor <*ipv6 address*> **system-control-evc**
neighbor <*ipv6 address*> **system-management-evc**

Syntax Description

<*ipv4 address*>	Specifies the IPv4 address for the BGP AF neighbor. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*ipv6 address*>	Specifies the IPv6 address for the BGP AF neighbor. IPv6 addresses should be expressed in colon hexadecimal format (for example, **2001:DB8:1::1**).
mef-ethernet <*slot/port*>	Optional. Specifies the BGP AF neighbor is the Metro Ethernet Forum (MEF) Ethernet interface.
system-control-evc	Optional. Specifies the BGP AF neighbor is a member of the system control Ethernet virtual connection (EVC).
system-management-evc	Optional. Specifies the BGP AF neighbor is a member of the system management EVC.

Default Values

By default, there are no configured BGP AF neighbors.

Command History

Release 11.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 addressing.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R10.11.0	Command was expanded to include the MEF Ethernet interface.

Functional Notes

The **neighbor** command can be used to specify the BGP AF neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures an IPv4 BGP AF neighbor with an IPv4 address of **10.10.10.1** on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 10.10.10.1**

The following example configures an IPv4 BGP AF neighbor with an IPv4 address of **10.10.10.1** on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.10.10.1**

network *<ipv4 address>* **mask** *<subnet mask>*

Use the **network mask** command to allow the Border Gateway Protocol (BGP) address family (AF) to advertise local networks that remote sites should be able to access. This command can be used for an Internet Protocol version 4 (IPv4) BGP AF on the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the configured network.

Syntax Description

<ipv4 address>	Specifies the network address for the neighbor that AOS will advertise over BGP. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks must be expressed in dotted decimal notation (for example, **255.255.255.0**).

Default Values

By default, there are no configured BGP networks.

Command History

Release 11.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **network** command can be used to specify the advertised routes for BGP AF neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example adds the **10.10.10.1** network with a subnet mask of **255.255.255.0** to the IPv4 BGP AF on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#network 10.10.10.1 mask 255.255.255.0**

The following example adds the **10.10.10.1** network with a subnet mask of **255.255.255.0** to the IPv4 BGP AF on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#network 10.10.10.1 mask 255.255.255.0**

network *<ipv6 address/prefix-length>*

Use the **network** command to allow the Border Gateway Protocol (BGP) address family (AF) to advertise local networks that remote sites should be able to access. This command can be used for an Internet Protocol version 6 (IPv6) BGP AF on the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to remove the configured network.

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 address and subnet for the neighbor that AOS will advertise over BGP. IPv6 addresses and prefixes should be expressed in colon hexadecimal format (for example, **2001:DB8:0:3F3B::/64**).

Default Values

By default, there are no configured BGP networks.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The **network** command can be used to specify the advertised routes for BGP AF neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv6 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher as-4byte 44:356**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv6**
(config-bgp-vrf-ipv6)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example adds the **2001:DB8:0:3F3B::/64** network to the IPv6 BGP AF on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv6**
(config-bgp-ipv6)**#network 2001:DB8:0:3F3B::/64**

The following example adds the **2001:DB8:0:3F3B::/64** network to the IPv6 BGP AF on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher as-4byte 44:356**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv6**
(config-bgp-vrf-ipv6)**#network 2001:DB8:0:3F3B::/64**

redistribute connected

Use the **redistribute connected** command to pass routes from one network to another, regardless of the routing protocol implemented on the routing domain. Using the **connected** keyword allows the propagation of routes connected to other interfaces using the Border Gateway Protocol (BGP) routing protocol for either the Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) BGP address family (AF) on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute connected
redistribute connected metric <*value*>
redistribute connected route-map <*name*>

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed connected routes in the BGP AF.
route-map <*name*>	Optional. Specifies the route map filter to use for advertising redistributed connected routes in the BGP AF.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **redistribute connected** command can be used to specify the hop count for advertised routes for BGP AF neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

BGP does not blindly broadcast out of all interfaces. Instead, the network statement tells which networks to include in BGP updates. The **redistribute connected** command simply covers all connected networks.

Usage Examples

The following example passes the connected routes found in the route table to other networks running the BGP routing protocol from the IPv4 BGP AF on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#redistribute connected**

The following example passes the connected routes found in the route table to other networks running the BGP routing protocol from the IPv4 BGP AF on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#redistribute connected**

redistribute ospf

Use the **redistribute ospf** command to redistribute routes from one protocol to another, regardless of the routing protocol implemented on the routing domain. Using the **ospf** keyword allows the propagation of Open Shortest Path First (OSPF) routes into Border Gateway Protocol (BGP) for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) BGP address families (AFs) on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute ospf
redistribute ospf <*process id*>
redistribute ospf <*process id*> **include-connected**
redistribute ospf <*process id*> **metric** <*value*>
redistribute ospf <*process id*> **no-include-connected**
redistribute ospf <*process id*> **route-map** <*map*>

After specifying the process id, the other parameters can be entered in any order. Use the ***?*** *after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

<*process id*>	Optional. Specifies the OSPFv2 or OSPFv3 routing process from which BGP AF routes will be redistributed. The process ID is locally significant to the device, and must be unique among OSPF processes of the same version on the device. Valid range is **1** to **65535**.
include-connected	Optional. Used for OSPFv3 and IPv6 BGP AFs to specify that prefixes of the interface running this source protocol are included in the route redistribution.
no-include-connected	Optional. Used for OSPFv2 and IPv4 BGP AFs to specify that prefixes of the interface running this source protocol are not automatically included in the route redistribution.
metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed OSPF routes in the BGP AF. When used with a process ID, it applies to IPv6 BGP AF only.
route-map <*map*>	Optional. Specifies the route map filter to use for advertising redistributed OSPF routes in the BGP AF.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Release R10.5.0	Command was expanded to include the <*process id*> and **include-connected** parameters. Command was also expanded to include IPv6 functionality.
Release R11.3.0	Command was expanded to include the <*process id*> parameter for OSPFv2 and the **no-include-connected** parameter.

Functional Notes

The **redistribute ospf** command can be used to specify the hop count for advertised OSPF routes for BGP AF neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Redistributing OSPF routes imports those routes into BGP without specifying those subnets with a network statement. The OSPF routes imported this way are not covered by a network command.

If **redistribute ospf** is enabled and no metric value is specified, the value defaults to **0**.

Usage Examples

The following example imports OSPF routes into the IPv4 BGP AF on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#redistribute ospf**

The following example imports OSPF routes into the IPv4 BGP AF on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#redistribute ospf**

redistribute rip

Use the **redistribute rip** command to redistribute routes from one protocol to another, regardless of the routing protocol implemented on the routing domain. Using the **rip** keyword allows the propagation of Routing Information Protocol (RIP) routes into Border Gateway Protocol (BGP) for the Internet Protocol version 4 (IPv4) BGP address family (AF) on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute rip
redistribute rip metric <*value*>
redistribute rip route-map <*name*>

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed RIP routes in the BGP AF.
route-map <*name*>	Optional. Specifies the route map filter to use for advertising redistributed RIP routes in the BGP AF.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **redistribute rip** command can be used to specify the hop count for advertised RIP routes for BGP AF neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Redistributing RIP routes imports those routes into BGP. The RIP routes imported this way are not covered by a network command.

If **redistribute rip** is enabled and no metric value is specified, the value defaults to **0**.

Usage Examples

The following example imports RIP routes into the IPv4 BGP AF on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#redistribute rip**

The following example imports RIP routes into the IPv4 BGP AF on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#redistribute rip**

redistribute static

Use the **redistribute static** command to pass routes from one network to another, regardless of the routing protocol implemented on the routing domain. Using the **static** keyword allows the propagation of static routes into the Border Gateway Protocol (BGP) routing protocol for both the Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) BGP address family (AF) on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute static
redistribute static metric <*value*>
redistribute static route-map <*name*>

The gateway network for the static route must participate in BGP by using the network command for the gateway network.

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed static routes in the BGP AF.
route-map <*name*>	Optional. Specifies the route map filter to use for advertising redistributed static routes in the BGP AF.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **redistribute static** command can be used to specify the hop count for advertised static routes for BGP AF neighbors on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**

(config-bgp-vrf-ipv4)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Redistributing static routes allows other network devices to learn about routes without requiring manual input to each device on the network.

Usage Examples

The following example passes the static routes found in the route table to other networks running the BGP routing protocol from the IPv4 BGP AF on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#redistribute static**

The following example passes the static routes found in the route table to other networks running the BGP routing protocol from the IPv4 BGP AF on the nondefault VRF instance named **RED1**:

config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#redistribute static**

BGP AF NEIGHBOR COMMAND SET

In AOS firmware release 18.03.00, Multiple virtual routing and forwarding (VRF) Border Gateway Protocol (BGP) functionality was incorporated into AOS. This release allows BGP configuration to occur on different VRF instances, and changes the hierarchical structure of BGP within AOS as well as the configuration steps necessary for BGP configuration. In addition, in AOS firmware release R10.1.0, support for multiprotocol BGP and Internet Protocol version 6 (IPv6) BGP were added.

The following are new features of BGP included with Multi-VRF BGP.

Address families (AFs) are used in BGP to maintain a separation between Internet protocol types within a VRF instance. With the advent of Multi-VRF BGP in 18.03.00, AOS implemented the use of AFs into the BGP hierarchical structure. An AF is a configuration structure that can reside at the default VRF instance and within a nondefault VRF instance. Creating an address family enables processing of that address family within a VRF, and it provides a place for AF-specific configuration.

In addition to the use of AFs, Multi-VRF BGP also allows the recognition and configuration of VRF instances specific to BGP functionality within the router. This allows the VRF constructs from the service provider to be incorporated into the customer router.

Multi-VRF is an application of the typical BGP functionality. As the name suggests, Multi-VRF BGP extends traditional service provider multi-VRF functionality of BGP to the customer edge router. This type of feature is typically used in Layer 3 virtual private network (VPN) applications where the VPN is extended to the customer device using multi-VRF. Multi-VRF BGP allows the customer edge router to dynamically exchange customer VPN routers to and through the provider's VPN *cloud*, thus eliminating the reliance on the provider to manage static routes. Multi-VRF takes place on the link between the service provider's routers and the customer edge equipment.

In Multi-VRF BGP the concepts of the address family and VRF instances are incorporated into the BGP configuration structure. VRF instances are in themselves not tied to a specific protocol, and therefore, control of multiple protocols within a single VRF is accomplished using an AF. Multi-VRF BGP also uses the concepts of AFs to provide specific BGP configuration to a single BGP policy, and maintain control over multiple bGP policies within a single AF.

In Multi-VRF BGP, the hierarchical structure of BGP configuration is as follows:

```
Global BGP settings (affecting all of BGP for this router)
!
VRF BGP settings (affecting only the default VRF)
Neighbor #1 Definition
    Neighbor #1 common settings (common to all peering with neighbor #1)
    exit
!
Address Family for the default VRF
    AF BGP settings (affecting only this AF)
    Neighbor #1 Reference
        Neighbor #1 AF-specific settings
```



```
        exit
    exit
!
VRF name1
    VRF BGP settings (affecting only this vRF)
    Neighbor #2 Definition
        Neighbor #2 common settings (common to all peering with neighbor #2)
        exit
!
Address Family for VRF name1
    AF BGP settings (affecting this AF)
    Neighbor #2 Reference
        Neighbor #2 settings specific to this AF
        exit
    exit
exit
```

Because the structure of BGP changed with the AOS 18.03.00 release, there are several sections of BGP configuration commands. The following are the BGP configuration command sections for AOS products, and are applicable to both the default and nondefault VRF instances:

- *BGP Command Set on page 3981*
- *BGP Address Family Command Set on page 4001*
- *BGP AF Neighbor Command Set on page 4022*
- *BGP Neighbor Command Set on page 4041*

Once you have enabled BGP in AOS products, you can enter the AF Neighbor Configuration mode by entering the **neighbor** command at the BGP AF Configuration mode prompt. To enter the IPv4 BGP AF Neighbor Configuration mode for the default VRF, enter the command as follows:

```
>enable
#configure terminal
(config)#router bgp 100
(config-bgp)#address-family ipv4
(config-bgp-ipv4)#neighbor 10.20.1.1
(config-bgp-ipv4-neighbor)#
```

To enter the IPv6 BGP AF Neighbor Configuration mode for the default VRF, enter the command as follows:

```
>enable
#configure terminal
(config)#router bgp 100
(config-bgp)#address-family ipv6
(config-bgp-ipv6)#neighbor 2001:DB8:1::1
(config-bgp-ipv6-neighbor)#
```


The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

advertisement-interval <value> on page 4025
as-path-list <name> on page 4027
distribute-list on page 4029
next-hop-self on page 4031
prefix-list <name> on page 4033
route-map <name> on page 4035
send-community standard on page 4037
soft-reconfiguration inbound on page 4039

advertisement-interval *<value>*

Use the **advertisement-interval** command to configure AOS to specify how long the Border Gateway Protocol (BGP) process waits before sending updates to this neighbor. This command can be used for both the Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) BGP address family (AF) neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the advertisement interval in seconds. Range is **0** to **600** seconds.

Default Values

By default, the advertisement interval is **30** seconds for external BGP AF neighbors and **5** seconds for internal BGP AF neighbors.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **advertisement-interval** command can be used to specify the wait time for a BGP AF neighbor on either the default or nondefault VRF instance. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

The **advertisement-interval** command sets the minimum interval between sending updates to the specified neighbor.

Usage Examples

The following example configures the BGP process to wait at least **100** seconds before sending updates to this IPv4 AF neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#advertisement-interval 100**

The following example configures the BGP process to wait at least **100** seconds before sending updates to this IPv4 AF neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#advertisement-interval 100**

as-path-list *<name>*

Use the **as-path-list** command to assign a predefined autonomous system (AS) path list to a Border Gateway Protocol (BGP) Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) address family (AF) neighbor. This list is then used to filter inbound and/or outbound BGP route updates. This command can be used for a BGP AF neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to discontinue use of the list. Variations of this command include:

as-path-list <*name*> **in**
as-path-list <*name*> **out**

Syntax Description

<name>	Assigns an AS path list to this BGP AF neighbor.
in	Specifies the filtering of all inbound BGP route updates.
out	Specifies the filtering of all outbound BGP route updates.

Default Values

By default, no AS path lists are specified for filtering.

Command History

Release 9.3	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **as-path-list** command can be used to specify the AS path list for a BGP AF neighbor on either the default or nondefault VRF instance. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Before they can be assigned to a neighbor, AS path lists must first be defined using the command *ip classless on page 1348*.

Usage Examples

The following example uses the **no15** AS path list to filter all inbound BGP route updates for the IPv4 BGP AF neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#as-path-list no15 in**

The following example uses the **no15** AS path list to filter all inbound BGP route updates for the IPv4 BGP AF neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#as-path-list no15 in**

distribute-list

Use the **distribute-list** command to add route filtering functionality by assigning inbound and outbound Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) access control lists (ACLs) to a BGP address family (AF) neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance. Only one inbound/outbound pair of ACLs can be configured for a particular AF neighbor. Use the **no** form of this command to disable filtering. Variations of this command include:

distribute-list <*ipv4 acl name*> **in**
distribute-list <*ipv4 acl name*> **out**
distribute-list <*ipv6 acl name*> **in**
distribute-list <*ipv6 acl name*> **out**

For a complete list of all extended and standard ACL configuration commands, refer to the *IPv6 Access Control List Command Set on page 4296* or *IPv4 Access Control List Command Set on page 4252*.

Syntax Description

<ipv4 acl name>	Specifies an IPv4 ACL name. This is a standard IPv4 ACL against which the contents of the incoming/outgoing routing updates are matched.
<ipv6 acl name>	Specifies an IPv6 ACL name. This is a standard IPv6 ACL against which the contents of the incoming/outgoing routing updates are matched.
in	Applies route filtering to inbound data.
out	Applies route filtering to outbound data.

Default Values

By default, distribute-list filtering is disabled.

Command History

Release 12.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **distribute-list** command can be used to specify the IPv4 or IPv6 ACL used by a BGP AF neighbor on either the default or nondefault VRF instance. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**

(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example will filter out all network advertisements received by the IPv4 BGP AF neighbor on the default VRF instance via Ethernet interface **0/1** with the exception of the **10.10.10.0** network:

(config)**#ip access-list standard TRUSTED**
(config-std-nacl)**#permit 10.10.10.0 0.0.0.255**
(config-std-nacl)**#exit**
(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#distribute-list TRUSTED in**

The following example will filter out all network advertisements received by the IPv4 BGP AF neighbor on the nondefault VRF instance named **RED1** via Ethernet interface **0/1** with the exception of the **10.10.10.0** network:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#distribute-list TRUSTED in**

next-hop-self

Use the **next-hop-self** command to force the NEXT_HOP attribute to be changed to this unit's IP address for each network it advertises to the Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) BGP address family (AF) neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled and the next autonomous system (AS) is advertised as the NEXT_HOP attribute.

Command History

Release 9.3	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **next-hop-self** command can be used to specify the IPv4 address used by a BGP AF neighbor on either the default or nondefault VRF instance. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Internal Gateway Protocols (IGPs), such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), always use the source IP address of a routing update as the next-hop address for each network that is placed in the routing table. Conversely, since BGP routes AS-to-AS, the default next hop that is advertised is the next AS. This behavior can present a problem in situations where an internal Border Gateway Protocol (iBGP) router learns about networks outside of its AS through one of its iBGP peers. By default, the next-hop address for the external networks advertised to the iBGP router is the entry

point for the next AS. When the iBGP router receives packets destined for one of the external networks, it performs a recursive lookup of the entries in its own IGP routing table to determine how to reach the BGP next-hop address. Unless the iBGP router has a static route or an entry in its IGP routing table indicating how to reach the edge router in the external AS, packets destined for those networks will be dropped. To remedy this scenario, the iBGP peer must advertise its own IP address as the next-hop address to the external networks. Consider the following example:

In external Border Gateway Protocol (eBGP), routes are normally advertised with a next hop set to the IP address that the receiving peer has configured in its neighbor statement for this router. In the eBGP case where the receiving router is in the same subnet as the current next hop, the current next hop is not changed.

For broadcast multiaccess networks (Ethernet), this provides more efficient routing. For nonbroadcast multiaccess (NBMA) networks, such as Frame Relay with a partial mesh using point-to-multipoint circuits, this rule can cause significant problems. Since the partial mesh is on the same subnet, BGP applies the rule of not changing the next-hop address, rendering routes in certain topologies invalid. This is one case where this command is necessary to solve a problem.

Usage Examples

The following example enables **next-hop-self** for the IPv4 BGP AF neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#next-hop-self**

The following example enables **next-hop-self** for the IPv4 BGP AF neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#next-hop-self**

prefix-list <*name*>

Use the **prefix-list** command to assign a predefined prefix list to an Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) address family (AF) neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance. The list is then used to filter BGP route updates received and/or sent from/by the specified peer. Use the **no** form of this command to discontinue use of the prefix list. Variations of this command include:

prefix-list <*name*> **in**
prefix-list <*name*> **out**

Syntax Description

<*name*>	Assigns the specified prefix list to this BGP AF neighbor.
in	Specifies that all inbound BGP route updates received from the specified peer be filtered.
out	Specifies that all outbound BGP route updates being sent to the specified peer be filtered.

Default Values

By default, no prefix lists are specified for filtering.

Command History

Release 9.3	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **prefix-list** command can be used to specify the prefix list used by a BGP AF neighbor on either the default or nondefault VRF instance. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Before they can be assigned to a BGP AF neighbor, prefix lists must first be defined using the **ip prefix-list** <*name*> **seq** <*number*> or **ipv6 prefix-list** <*name*> **seq** <*number*> command. Refer to the command *ip prefix-list <name> seq <number> on page 1443* or *ipv6 prefix-list <name> seq <number> on page 1556* for more information.

Usage Examples

The following example uses the **MyList** prefix list to filter all BGP updates received by the IPv4 BGP AF neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#prefix-list MyList in**

The following example uses the **MyList** prefix list to filter all BGP updates received by the IPv4 BGP AF neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#prefix-list MyList in**

route-map <*name*>

Use the **route-map** command to assign a route map to this Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) address family (AF) neighbor. You can apply the route map to BGP AF neighbors on either the default or nondefault virtual routing and forwarding (VRF) instance. The route map is then used to filter or modify inbound and/or outbound BGP route updates. Use the **no** form of this command to return to the default setting. Variations of this command include:

route-map <*name*> **in**
route-map <*name*> **out**

Syntax Description

<*name*>	Assigns the specified route map to this BGP AF neighbor.
in	Specifies the filtering/modification of all inbound BGP route updates.
out	Specifies the filtering/modification of all outbound BGP route updates.

Default Values

By default, no route map is assigned.

Command History

Release 9.3	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **route-map** command can be used to specify the route map used by a BGP AF neighbor on either the default or nondefault VRF instance. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Before a route map can be assigned to a BGP neighbor, it must first be defined using the command *route-map on page 1687*.

Usage Examples

The following example assigns a route map to the IPv4 BGP AF neighbor on the default VRF instance for outbound filtering:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#route-map MapName out**

The following example assigns a route map to the IPv4 BGP AF neighbor on the nondefault VRF instance named **RED1** for outbound filtering:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#route-map MapName out**

send-community standard

Use the **send-community standard** command to insert a standard Border Gateway Protocol (BGP) community attribute to all outgoing route updates for this Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) BGP address family (AF) neighbor. You can insert a BGP community attribute to the BGP AF neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 9.3	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **send-community standard** command can be used to specify the BGP community used by a BGP AF neighbor on either the default or nondefault VRF instance. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example inserts a standard BGP community attribute to all outgoing route updates for the IPv4 BGP AF neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#send-community standard**

The following example inserts a standard BGP community attribute to all outgoing route updates for the IPv4 BGP AF neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#send-community standard**

soft-reconfiguration inbound

Use the **soft-reconfiguration inbound** command to enable this unit to store all updates from an Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) address family (AF) neighbor in case the inbound policy is changed. This command can be used for a BGP AF neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 9.3	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.1.0	Command was expanded to include IPv6 functionality.

Functional Notes

The **soft-reconfiguration inbound** command can be used to specify that a BGP AF neighbor on either the default or nondefault VRF instance store all updates. If the AF neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP AF neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the IPv4 BGP AF neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

The **soft-reconfiguration inbound** command allows a network administrator to reconfigure BGP policies without clearing active BGP sessions. Administrators can then institute new policies at any time without forcing the neighbors to re-establish their connection and possibly disrupting traffic.

BGP updates are stored prior to filtering; thus, allowing the **clear bgp soft** command to be used in the absence of route refresh (RFC 2918) capability. The unfiltered table is used when an inbound policy is changed; allowing the router to immediately implement policy changes immediately based on the stored table instead of having to wait on a new table to be built after a hard reset. A soft reset is beneficial over a hard reset because it allows policy updates without disrupting network traffic flow. A hard reset terminates the existing BGP session, effectively removing all routes learned from a neighbor. A new session is then created and all of the routes must be relearned. Due to the fact that this process takes place with a hard reset, a network outage can potentiality occur until the BGP database and route table have been rebuilt.

Refer to *clear bgp on page 107* for more information.

Usage Examples

The following example enables the unit to store BGP updates for the IPv4 BGP AF neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#address-family ipv4**
(config-bgp-ipv4)**#neighbor 192.22.73.101**
(config-bgp-ipv4-neighbor)**#soft-reconfiguration inbound**

The following example enables the unit to store BGP updates for the IPv4 BGP AF neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#address-family ipv4**
(config-bgp-vrf-ipv4)**#neighbor 10.20.1.1**
(config-bgp-vrf-ipv4-neighbor)**#soft-reconfiguration inbound**

BGP NEIGHBOR COMMAND SET

Border Gateway Protocol (BGP) differs from many routing protocols because it does not allow a router to automatically search for peers from which to obtain routes. A separate BGP neighbor must be manually configured for each router with which the local router will communicate. Optional filtering policies can be configured for individual neighbors and are used by the router to dictate which routes the BGP interface sends to and accepts from the neighbor. In AOS firmware release 18.03.00, Multi-VRF BGP functionality was incorporated into AOS. This release allows BGP configuration to occur on different VRF instances, and changes the hierarchical structure of BGP within AOS as well as the configuration steps necessary for BGP configuration. In addition, in AOS firmware release R10.1.0, support for multiprotocol BGP and Internet Protocol version 6 (IPv6) BGP were added.

The following are new features of BGP included with Multi-VRF BGP.

Address families (AFs) are used in BGP to maintain a separation between Internet protocol types within a VRF instance. With the advent of Multi-VRF BGP in 18.03.00, AOS implemented the use of AFs into the BGP hierarchical structure. An AF is a configuration structure that can reside at the default VRF instance and within a nondefault VRF instance. Creating an address family enables processing of that address family within a VRF, and it provides a place for AF-specific configuration.

In addition to the use of AFs, Multi-VRF BGP also allows the recognition and configuration of VRF instances specific to BGP functionality within the router. This allows the VRF constructs from the service provider to be incorporated into the customer router.

Multi-VRF is an application of the typical BGP functionality. As the name suggests, Multi-VRF BGP extends traditional service provider multi-VRF functionality of BGP to the customer edge router. This type of feature is typically used in Layer 3 virtual private network (VPN) applications where the VPN is extended to the customer device using multi-VRF. Multi-VRF BGP allows the customer edge router to dynamically exchange customer VPN routers to and through the provider's VPN *cloud*, thus eliminating the reliance on the provider to manage static routes. Multi-VRF takes place on the link between the service provider's routers and the customer edge equipment.

In Multi-VRF BGP the concepts of the address family and VRF instances are incorporated into the BGP configuration structure. VRF instances are in themselves not tied to a specific protocol, and therefore, control of multiple protocols within a single VRF is accomplished using an AF. Multi-VRF BGP also uses the concepts of AFs to provide specific BGP configuration to a single BGP policy, and maintain control over multiple BGP policies within a single AF.

In Multi-VRF BGP, the hierarchical structure of BGP configuration is as follows:

```
Global BGP settings (affecting all of BGP for this router)
!
VRF BGP settings (affecting only the default VRF)
Neighbor #1 Definition
    Neighbor #1 common settings (common to all peering with neighbor #1)
    exit
!
```



```
Address Family for the default VRF
    AF BGP settings (affecting only this AF)
    Neighbor #1 Reference
        Neighbor #1 AF-specific settings
        exit
    exit
!
VRF name1
    VRF BGP settings (affecting only this vRF)
    Neighbor #2 Definition
        Neighbor #2 common settings (common to all peering with neighbor #2)
        exit
!
Address Family for VRF name1
    AF BGP settings (affecting this AF)
    Neighbor #2 Reference
        Neighbor #2 settings specific to this AF
        exit
    exit
exit
```

Because the structure of BGP changed with the AOS 18.03.00 release, there are several sections of BGP configuration commands. The following are the BGP configuration command sections for AOS products, and are applicable to both the default and nondefault VRF instances:

- *BGP Command Set on page 3981*
- *BGP Address Family Command Set on page 4001*
- *BGP AF Neighbor Command Set on page 4022*
- *BGP Neighbor Command Set on page 4041*

To activate the BGP Neighbor Configuration mode, enter the **neighbor** command at the BGP Configuration mode prompt followed by the neighbor's IP address.

The IP address entered in this command must match the address for the interface that the remote router is using as its update source.

The local router must be able to reach the IP address configured as the neighbor ID. View the routing table and verify that it includes a route to this address.

Enter the IPv4 BGP Neighbor Configuration mode from the BGP Configuration mode as follows (for the default VRF instance):

```
>enable
#configure terminal
(config)#router bgp 1
(config-bgp)#neighbor 192.22.73.101
(config-bgp-neighbor)#
```

Enter the IPv6 BGP Neighbor Configuration mode from the BGP Configuration mode as follows (for the default VRF instance):

```
>enable
#configure terminal
(config)#router bgp 1
(config-bgp)#neighbor 2001:DB8:1::1
(config-bgp-neighbor)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

ebgp-multihop <value> on page 4044
hold-timer <value> on page 4046
local-as <value> on page 4048
password <password> on page 4050
remote-as <value> on page 4052
transport connection-mode on page 4054
update-source on page 4056

ebgp-multihop *<value>*

Use the **ebgp-multihop** command to configure the maximum hop count of Border Gateway Protocol (BGP) messages to a neighbor. This command can be applied to either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the maximum hop count of BGP messages to a neighbor. Range is **1** to **255** hops.

Default Values

By default, BGP multihop is set to **1**.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **ebgp-multihop** command can be used to allow a BGP neighbor on a network that is not directly connected on either the default or nondefault VRF instance. If the behavior is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

The **ebgp-multihop** command allows a BGP neighbor to be on a network that is not directly connected. Normally, BGP peers are directly connected. In certain applications, a non-BGP device, such as a firewall or router, can reside between BGP peers. In this case, the **ebgp-multihop** command is required to allow updates to have a time to live (TTL) greater than 1 and to allow received BGP updates to be added to the BGP table when the next-hop address is not directly connected.

Usage Examples

The following example allows a BGP message on the default VRF instance to travel **10** hops to a neighbor:

(config)**#router bgp 100**
(config-bgp)**#neighbor 192.22.73.101**
(config-bgp-neighbor)**#ebgp-multihop 10**

The following example allows a BGP message on the nondefault VRF instance named **RED1** to travel **10** hops to a neighbor:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)**#ebgp-multihop 10**

hold-timer <*value*>

Use the **hold-timer** command to set the default hold time for the Border Gateway Protocol (BGP) neighbor on either the default or nondefault virtual routing and forwarding (VRF) instance.

Syntax Description

<*value*>	Specifies a time interval (in seconds) within which a keepalive must be received from a peer before that peer is declared dead. Range is **0** to **65535** seconds.

Default Values

By default, the hold time is **180** seconds.

Command History

Release 8.1	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **hold-timer** command can be used to specify the hold timer for the BGP neighbor on either the default or nondefault VRF instance. If the neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Using the **hold-timer** command in BGP Neighbor Configuration mode sets the hold time for only that neighbor. The peers will negotiate and use the lowest configured setting. The keepalive interval will be set to one-third of the negotiated hold time.

Usage Examples

The following example sets a hold time of **120** seconds for this BGP neighbor, with an understood keepalive interval of **40** seconds, on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#neighbor 10.20.1.1**
(config-bgp-neighbor)**#hold-timer 120**

The following example sets a hold time of **120** seconds for this BGP neighbor, with an understood keepalive interval of **40** seconds, on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)**#hold-timer 120**

local-as <*value*>

Use the **local-as** command to specify an autonomous system (AS) number for the unit to use when communicating with this Border Gateway Protocol (BGP) neighbor. This command can be used for BGP neighbors on either the default or nondefault virtual routing and forwarding (VRF) instances. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the AS number to use when communicating with this neighbor. Must be different than the AS number for this router and the peer router. Only valid for external Border Gateway Protocol (eBGP) connections. Range is **0** to **4294967295**. When **0** is sued, it indicates that the BGP process local AS is used, because **0** is not a valid AS number.

Default Values

By default, the **local-as** value is set to **0**, indicating the router's BGP AS number is used.

Command History

Release 9.3	Command was introduced.
Release 18.1	Command was altered to support 4-byte AS numbers (previously AOS only supported 2-byte numbers).
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **local-as** command can be used to specify the AS number for the unit to use when communicating with this BGP neighbor on either the default or nondefault VRF instance. If the neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

The **local-as** command substitutes a different AS number to be used for communicating with this BGP neighbor (other than the one the router is actually a member of). This can be used to satisfy network designs requiring a customer to appear as one AS number when communicating with one Internet service provider (ISP) and another when communicating with another ISP.

Usage Examples

The following example configures this BGP neighbor's AS number on the default VRF instance to be **300**:

(config)**#router bgp 100**
(config-bgp)**#neighbor 192.22.73.101**
(config-bgp-neighbor)**#local-as 300**

The following example configures this BGP neighbor's AS number on the nondefault VRF instance named **RED1** to be **300**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)**#local-as 300**

Technology Review

This router appears (to the peer router) to be in the AS specified with the **local-as** command. Therefore, all routes learned from the peer have this number prepended to the AS path. In network advertisements from routers using the **local-as** command, the router's true AS number (the number specified using the **router bgp as-number** command) is prepended to the AS path attribute, and the local AS (the number specified in the **neighbor local-as** command) is prepended to the AS path attribute. This makes it appear that the path to the network is first through the local AS, and then through the true AS. To further illustrate, consider the following example network.

In this network:

- Router A is in AS 100.
- Router B is in AS 300.
- Router A is an eBGP peer with Router B.
- Router A's connection to Router B specifies a **local-as** of 200.
- Router B is configured to connect to Router A in AS 200.

Therefore:

- To Router B, all aspects of Router A appear as AS 200.
- Networks advertised from Router A to Router B will have the AS path **200 100** prepended to the AS path attribute.
- Router A will add AS 200 to the AS path of networks learned from Router B.

password *<password>*

Use the **password** command to enable message digest 5 (MD5) password authentication on Transmission Control Protocol (TCP) segments exchanged with the Border Gateway Protocol (BGP) peer. This command can be used for BGP neighbors on the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to disable authentication.

Syntax Description

<password>	Specifies the password string to be used for authentication. The password is case sensitive and must not exceed **80** characters.

Default Values

By default, authentication is disabled.

Command History

Release 9.3	Command was introduced.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **password** command can be used to specify the authentication password used for TCP communication with this BGP neighbor on either the default or nondefault VRF instance. If the neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Authentication must be configured on both peers using the same password. Every BGP TCP segment sent is authenticated. Configuring authentication causes an existing session to be torn down and re-established using the currently specified authentication.

Usage Examples

The following example enables authentication for this BGP neighbor on the default VRF instance and sets a password of **user1**:

(config)**#router bgp 100**
(config-bgp)**#neighbor 192.22.73.101**
(config-bgp-neighbor)**#password user1**

The following example enables authentication for this BGP neighbor on the nondefault VRF instance named **RED1** and sets a password of **user1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)**#password user1**

remote-as <*value*>

Use the **remote-as** command to specify the Border Gateway Protocol (BGP) autonomous system (AS) to which the neighbor belongs, adding an entry to the BGP neighbor table. This command can be used for BGP neighbors on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the AS number. This number must be different from the AS number of the local router (defined using the command *router bgp <value> on page 1689*). Range is **1** to **4294967295**.

Default Values

By default, no BGP neighbors are defined.

Command History

Release 9.3	Command was introduced.
Release 18.1	Command was altered to support 4-byte AS numbers (previously AOS only supported 2-byte numbers).
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.

Functional Notes

The **remote-as** command can be used to specify the AS number for this BGP neighbor on either the default or nondefault VRF instance. If the neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures a remote AS number of **200** for this neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#neighbor 192.22.73.101**
(config-bgp-neighbor)**#remote-as 200**

The following example configures a remote AS number of **200** for this neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)**#remote-as 200**

transport connection-mode

Use the **transport connection-mode** command to specify Border Gateway Protocol (BGP) transport session options for the BGP neighbor. This command can be used for BGP neighbors on the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return the connection mode to the default value. Variations of this command include:

transport connection-mode active
transport connection-mode passive

Syntax Description

active	Specifies that only active Transmission Control Protocol (TCP) session connections are allowed for this neighbor. Active connections are those that are initiated by the router to establish a TCP connection to the neighbor.
passive	Specifies that only passive TCP session connections are allowed for this neighbor. Passive connections are those in which the router is only allowed to listen for incoming BGP connections without trying to establish a connection.

Default Values

By default, both active and passive connections are supported simultaneously, and a collision detection algorithm is used to determine which TCP session to use should an inbound and outbound connection begin.

Command History

Release 18.3	Command was introduced.

Functional Notes

The **transport connection-mode** command can be used to specify the connection mode for this BGP neighbor on either the default or nondefault VRF instance. If the neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that **active** connections are allowed for this BGP neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#neighbor 192.22.73.101**
(config-bgp-neighbor)**#transport connection-mode active**

The following example specifies that **active** connections are allowed for this BGP neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)**#transport connection-mode active**

update-source

Use the **update-source** command to specify which interface's IPv4 address will be used as the source IPv4 address for the Border Gateway Protocol (BGP) Transmission Control Protocol (TCP) connection (when connecting to this peer). This command can be used for BGP neighbors on either the default or nondefault virtual routing and forwarding (VRF) instance. Use the **no** form of this command to return to the default setting. Variations of this command include:

update-source <*interface*>
update-source system-control-evc
update-source system-management-evc

Syntax Description

<*interface*>	Specifies the interface to be used as the source IPv4 address. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**. Type **update-source ?** for a complete list of valid interfaces.
system-control-evc	Specifies the system control Ethernet virtual connection (EVC) is used as the source IPv4 address.
system-management-evc	Specifies the system management EVC is used as the source IPv4 address.

Default Values

By default, the outbound interface's IPv4 address is used for BGP updates.

Command History

Release 9.3	Command was introduced.
Release 14.1	Command was expanded to include the asynchronous transfer mode (ATM) and high level data link control (HDLC) interfaces.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release 18.3	Command was incorporated into Multi-VRF BGP functionality.
Release R10.4.0	Command was expanded to include the virtual local area network (VLAN) interface.
Release R10.10.0	Command was expanded to include the system control and system management EVCs.
Release R11.3.0	Command was expanded to include the Ethernet in the first mile (EFM) group interface.

Functional Notes

The **update-source** command can be used to specify the source IP address for this BGP neighbor on either the default or nondefault VRF instance. If the neighbor is to be created on a nondefault VRF instance, the VRF instance must first be created using the command *vrf <name> route-distinguisher on page 1989*. Once you have created the nondefault VRF instance, you can configure the BGP neighbor settings for the VRF instance using the command *vrf <name> on page 4000* from the router's BGP Configuration mode. For example, to configure the BGP neighbor characteristics for the nondefault VRF instance **RED1**, enter the following commands:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)#

For more information about VRF and Multi-VRF BGP configuration, refer to the configuration guides *Configuring IPv4 Multi-VRF in AOS* and *Configuring BGP in AOS for Releases 18.03.00/R10.1.0 or Later* available online at https://supportcommunity.adtran.com.

The source interface is most often configured as a loopback interface that is reachable by the peer router. The peer will specify this address in its neighbor commands for this router.

Usage Examples

The following example configures the **loopback 1** interface as the source IPv4 address for this BGP neighbor on the default VRF instance:

(config)**#router bgp 100**
(config-bgp)**#neighbor 192.22.73.101**
(config-bgp-neighbor)**#update-source loopback 1**

The following example configures the **loopback 1** interface as the source IPv4 address for this BGP neighbor on the nondefault VRF instance named **RED1**:

(config)**#vrf RED1 route-distinguisher ip 192.17.250.24:33**
(config)**#router bgp 100**
(config-bgp)**#vrf RED1**
(config-bgp-vrf)**#neighbor 10.20.1.1**
(config-bgp-vrf-neighbor)**#update-source loopback 1**

COMMUNITY LIST COMMAND SET

To activate the Community List Configuration mode, enter the **ip community-list** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip community-list listname
(config-comm-list)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

deny on page 4059
permit on page 4060

deny

Use the **deny** command to add an entry to the community list that denies Border Gateway Protocol (BGP) routes containing the specified community number in the community attribute. Use the **no** form of this command to remove the statement from the community list. Variations of this command include:

deny <*value*>
deny internet
deny local-as
deny no-advertise
deny no-export

Syntax Description

<*value*>	Denies routes that contain this value in their community attribute. This is a numeric value that can be an integer from **1** to **4294967295** or string in the form ***aa:nn***, where ***aa*** is the autonomous system (AS) number and ***nn*** is the community number. Multiple community number parameters can be present in the command.
internet	Denies routes that contain the reserved community number for the Internet community.
local-as	Denies routes that contain the reserved community number for NO_EXPORT_SUBCONFED. Routes containing this attribute should not be advertised to external BGP peers.
no-advertise	Denies routes that contain the reserved community number for NO_ADVERTISE. Routes containing this attribute should not be advertised to any BGP peer.
no-export	Denies routes that contain the reserved community number for NO_EXPORT. Routes containing this attribute should not be advertised to BGP peers outside a confederation boundary.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example creates a community list named **MyList** to deny BGP routes that have the Internet community number in their community attribute:

(config)**#ip community-list MyList**
(config-comm-list)**#deny no-export**

permit

Use the **permit** command to add an entry to the community list that allows only Border Gateway Protocol (BGP) routes containing the specified community number in the community attribute. Use the **no** form of this command to remove the statement from the community list. Variations of this command include:

permit <*value*>
permit internet
permit local-as
permit no-advertise
permit no-export

Syntax Description

<*value*>	Permits routes that contain this value in their community attribute. This is a numeric value that can be an integer from **1** to **4294967295** or string in the form ***aa:nn***, where ***aa*** is the autonomous system (AS) number and ***nn*** is the community number. Multiple community number parameters can be present in the command.
internet	Permits routes that contain the reserved community number for the Internet community.
local-as	Permits routes that contain the reserved community number for NO_EXPORT_SUBCONFED. Routes containing this attribute should not be advertised to external BGP peers.
no-advertise	Permits routes that contain the reserved community number for NO_ADVERTISE. Routes containing this attribute should not be advertised to any BGP peer.
no-export	Permits routes that contain the reserved community number for NO_EXPORT. Routes containing this attribute should not be advertised to BGP peers outside a confederation boundary.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example permits BGP routes that match the AS path attributes:

(config)**#ip as-path-list listname**
(config-comm-list)**#permit 30:22**

NETWORK MONITORING COMMAND SETS

This section includes the following command sets:

NETWORK MONITOR PROBE COMMAND SET

This section explains the commands available for Network Monitoring Probes. Probes are software agents that send test traffic across a network path. Tracks are standalone objects that can help determine the status of a route based on the success or failure of a probe. The probes can be configured to trigger at particular intervals. There are five types of probes supported by Adtran Operating System (AOS): Internet Control Message Protocol (ICMP) echo, Transmission Control Protocol (TCP) connect, Hypertext Transfer Protocol (HTTP) request, Two-Way Active Measurement Protocol (TWAMP), and ICMP timestamp. Commands common to all the probe types are identified in the following section, as well as isolated commands that only apply to the specific probe types.

Additional configuration commands are available for associating tracks with each probe. These are explained in the *Network Monitor Track Command Set on page 4098*.

To activate the Network Monitor Probe Configuration mode, enter the **probe** command at the Global Configuration mode prompt followed by the probe name. Specify the probe type of **icmp-echo**, **tcp-connect**, **http-request, icmp-timestamp**, and **twamp**. For example:

```
>enable
#configure terminal
(config)#probe probe1 icmp-echo
(config-probe-probe1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

The following commands are applicable to ICMP echo probe types and can be executed after this command:

(config)**#probe** <*probe name*> **icmp-echo**

data <pattern> on page 4069
destination on page 4070
period <value> on page 4076
size <payload length> on page 4079
source-address <ip address> on page 4080
timeout <value> on page 4084
tolerance on page 4085
vrf <name> on page 4088

The following commands are applicable to TCP connect probe types and can be executed after this command:

(config)#**probe** <*probe name*> **tcp-connect**

destination on page 4070
num-packets <value> on page 4075
period <value> on page 4076
source-address <ip address> on page 4080
source-port <port> on page 4081
timeout <value> on page 4084
tolerance on page 4085
vrf <name> on page 4088

The following commands are applicable to HTTP request probe types and can be executed after this command:

(config)#**probe** <*probe name*> **http-request**

absolute-path <name> on page 4065
destination on page 4070
expect regex <expression> on page 4072
expect status <minimum> <maximum> on page 4073
num-packets <value> on page 4075
period <value> on page 4076
raw-string on page 4077
source-address <ip address> on page 4080
source-port <port> on page 4081
timeout <value> on page 4084
tolerance on page 4085
type on page 4087
vrf <name> on page 4088

The following commands are applicable to ICMP timestamp probe types and can be executed after this command:

(config)#**probe** <*probe name*> **icmp-timestamp**

data on page 4068
destination on page 4070
dscp <value> on page 4071
history-depth <value> on page 4074
num-packets <value> on page 4075

num-packets <value> on page 4075
period <value> on page 4076
send-schedule periodic <value> on page 4078
size <payload length> on page 4079
source-address <ip address> on page 4080
threshold on page 4082
timeout <value> on page 4084
tolerance on page 4085
vrf <name> on page 4088

The following commands are applicable to TWAMP probe types and can be executed after this command:

(config)**#probe** <*probe name*> **twamp**

auth-mode open on page 4066
control on page 4067
data on page 4068
destination on page 4070
dscp <value> on page 4071
history-depth <value> on page 4074
num-packets <value> on page 4075
num-packets <value> on page 4075
period <value> on page 4076
send-schedule periodic <value> on page 4078
size <payload length> on page 4079
source-address <ip address> on page 4080
source-port <port> on page 4081
threshold on page 4082
timeout <value> on page 4084
tolerance on page 4085
vrf <name> on page 4088

absolute-path *<name>*

Use the **absolute-path** command to specify the server's root path. Use the **no** form of this command to return to the default setting.

Syntax Description

<name>	Specifies a path name.

Default Values

By default, the path name is the forward slash symbol (**/**).

Command History

Release 13.1	Command was introduced.

Functional Notes

This command can only be executed while in the **probe** *<name>* **http-request** command set.

Usage Examples

The following example sets the absolute path to **/home/index.html**:

(config)**#probe probe1 http-request**
(config-probe-probe1)**#absolute-path/home/index.html**

auth-mode open

Use the **auth-mode open** command to specify the authentication mode the probe must use for communication. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the authentication mode is **open**.

Command History

Release 17.2	Command was introduced.

Functional Notes

This command can only be executed while in the **probe** <*name*> **twamp** command set.

Usage Examples

The following example sets the authentication mode to **open**:

(config)**#probe probe1 twamp**
(config-probe-probe1)**#auth-mode open**

control

Use the **control** command to specify source and destination ports. Use the **no** form of this command to return to the default setting. Variations of this command include:

control dest-port owamp-control
control dest-port twamp-control
control dest-port <*port*>
control source-port <*port*>

Syntax Description

dest-port	Specifies the type of destination control port.
owamp-control	Specifies the destination One-Way Active Measurement Protocol (OWAMP) control port (861).
twamp-control	Specifies the destination Two-Way Active Measurement Protocol (TWAMP) default control port (862).
<*port*>	Specifies a destination TWAMP control port other than the default port 862. The valid range is **1** to **65535**.
source-port <*port*>	Specifies the TWAMP source control port. The valid range is **0** to **65535**.

Default Values

By default, the source port is **0**, which means that the source port will be dynamically selected by the probe. The default destination port is the TWAMP control port, port **862**.

Command History

Release 17.2	Command was introduced.
Release 17.6	Command was expanded to include the **twamp-control** parameter and default destination port was set to port **862**.

Functional Notes

This command can only be executed while in the **probe** <*name*> **twamp** command set.

Usage Examples

The following example specifies a destination control port for the **probe1** probe:

(config)**#probe probe1 twamp**
(config-probe-probe1)**#control dest-port owamp-control**

data

Use the **data** command to specify the data for padding a measurement packet. Payload data specifies the data used to pad a measurement packet. Payload data can consist of all zeros pattern, a random pattern, or a user-defined pattern. If the payload size is greater than the length of the pattern, the pattern will be repeated. Use the **no** form of this command to return to the default setting. Variations of this command include:

data pattern ascii <*string*>
data pattern hex <*string*>
data random
data zero

Syntax Description

pattern ascii <*string*>	Specifies an ASCII data pattern.
pattern hex <*string*>	Specifies a hexadecimal data pattern.
random	Specifies using a pattern of random numbers.
zero	Specifies using a pattern of zeros.

Default Values

By default, the data pattern is set to **zero**.

Command History

Release 17.2	Command was introduced to function with Two-Way Active Measurement Protocol (TWAMP) and Internet Control Message Protocol (ICMP) timestamp probes only.

Functional Notes

This command can only be executed while in the **probe** <*name*> **twamp** and **probe** <*name*> **icmp-timestamp** command set.

Usage Examples

The following example specifies a data pattern as **random**:

(config)**#probe probe2 twamp**
(config-probe-probe2)**#data random**

data *<pattern>*

Use the **data** command to specify a hexadecimal pattern to repeat in the Internet Control Message Protocol (ICMP) packet data section. Use the **no** form of this command to return to the default setting.

Syntax Description

<pattern>	Specifies a hexadecimal data pattern.

Default Values

By default, the data pattern is a standard ping packet pattern of data values starting with 0x00, incrementing by one for the length of the packet. Refer to *ping on page 48* for more information on ping packet data patterns.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example specifies a data pattern of **0FF0** for **probe1**:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#data 0FF0**

destination

Use the **destination** command to specify the destination host name and port for the probe object. Use the **no** form of this command to remove the setting. Variations of this command include:

destination <*hostname*>
destination <*hostname*> **port** <*number*>
destination interface <*interface*>
destination <*ip address*>
destination <*ip address*> **port** <*number*>

The probe is not operational until a destination is defined.

Syntax Description

<*hostname*>	Specifies the IP host by name.
interface <*interface*>	Specifies an interface's gateway as the destination for an Internet Control Message Protocol (ICMP) probe object. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for a Frame Relay interface, use **fr 1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **destination interface ?** for a complete list of valid interfaces.
<*ip address*>	Specifies a valid IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
port <*number*>	Optional. Specifies port number. This feature is not used with icmp-echo probes. The valid range is **1** to **65535**.

Default Values

By default, there is no setting for this command.

Command History

Release 13.1	Command was introduced.
Release R12.3.0	Command expanded to include the **interface** parameter for ICMP probes.

Usage Examples

The following example specifies **www.adtran.com** as the host and **port 21** File Transfer Protocol (FTP) as the destination for the HTTP request probe, **probe1**:

(config)**#probe probe1 http-request**
(config-probe-probe1)**#destination www.adtran.com port 21**

dscp *<value>*

Use the **dscp** command to specify the differentiated services code point (DSCP) value placed in the test packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the DSCP value. The range is **0** to **63**.

Default Values

By default, the DSCP value is **0**.

Command History

Release 13.1	Command was introduced.
Release 17.2	Command was added to the Two-Way Active Measurement Protocol (TWAMP) and Internet Control Message Protocol (ICMP) timestamp probes.

Usage Examples

The following example specifies DSCP value to be placed in the probe:

(config)**#probe probe2 icmp-timestamp**
(config-probe-probe2)**#dscp 15**

expect regex *<expression>*

Use the **expect regex** command to configure the probe to expect a regular expression inside the contents of the Hypertext Transfer Protocol (HTTP) response message. If the regular expression does not match anything, the probe fails. Use the **no** form of this command to return to the default setting.

Syntax Description

<expression>	Specifies the expression to display.

Default Values

By default, no regular expression is defined.

Command History

Release 13.1	Command was introduced.

Functional Notes

This command can only be executed while in the **probe** *<name>* **http-request** command set.

Usage Examples

The following example only allows the **probe1** test to pass if the word **success** is found in the HTTP server response message:

(config)**#probe probe1 http-request**
(config-probe-probe1)**#expect regex success**

expect status <*minimum*> <*maximum*>

Use the **expect status** command to configure the probe to expect a specific status code in response to an Hypertext Transfer Protocol (HTTP) request message. If a different status code is returned, the probe fails. Use the **no** form of this command to return to the default setting. Variations of this command include:

expect status <*minimum*>
expect status <*minimum*> <*maximum*>

Syntax Description

<*minimum*>	Specifies a minimum number value for the status code. Valid range is **0** to **999**.
<*maximum*>	Optional. Specifies a maximum number to create a range of status codes. Valid range is **0** to **999**.

Default Values

By default, there is no setting for this command.

Command History

Release 13.1	Command was introduced.

Functional Notes

This command can only be executed while in the **probe** <*name*> **http-request** command set.

Specifying only a minimum value indicates only one value can match the status code. Entering a maximum value indicates a range of possible matches.

Usage Examples

The following example configures **probe1** to expect a status code of **200** (the status of a successful HTTP request):

(config)**#probe probe1 http-request**
(config-probe-probe1)**#expect status 200**

history-depth <*value*>

Use the **history-depth** command to specify the number of probe operation results allowed to be stored in the unit's memory. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the number of probe operation results to keep in the history memory. The range is **1** to **120**.

Default Values

By default, the **history-depth** value is set to **1**.

Command History

Release 17.2	Command was introduced.

Functional Notes

This command can only be executed while in the **probe** <*name*> **icmp-timestamp** or **probe** <*name*> **twamp** command set.

Usage Examples

The following example specifies the number of probe results that can be stored in the unit:

(config)**#probe probe2 icmp-timestamp**
(config-probe-probe2)**#history-depth 30**

num-packets *<value>*

Use the **num-packets** command to specify the number of packets to send and receive during a single probe operation. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the number of packets. Valid range is **1** to **1000** packets.

Default Values

By default, the **num-packets** is set to **10**.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example specifies sending **10** packets during the probe test:

(config)**#probe probe3 twamp**
(config-probe-probe3)**#num-packets 10**

period <*value*>

Use the **period** command to specify the time between probe test attempts. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the time (in seconds) between probe test attempts. Valid range is **1** to **65535** seconds.

Default Values

By default, the period between probe tests is **60** seconds.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example specifies **probe1** to initiate probe tests every **90** seconds:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#period 90**

raw-string

Use the **raw-string** command to enter text to appear in the data portion of a Hypertext Transfer Protocol (HTTP) request. Refer to *ping on page 512* for more details on the output text. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Functional Notes

This command can only be executed while in the **probe** <*name*> **http-request** command set. The type should be set to RAW. Refer to *tolerance on page 4085* for more information.

The following system variables can be used in the text:

$SYSTEM_NAME = The host name of the system.

$SYSTEM_SERIAL_NUMBER = The serial number of the system.

$SYSTEM_DESCRIPTION = The product name and part number of the system.

$SYSTEM_SOFTWARE_VERSION = The firmware version of the system.

Usage Examples

The following example configures a RAW HTTP request that attempts to access **update.php** on the Web server. This command could be useful if the server administrator creates a PHP script that logs network connectivity information. Additional information (the router name and its uptime) placed after **update.php** is sent to the HTTP server.

```
(config)#probe probe1 http-request
(config-probe-probe1)#raw-string
    GET /update.php?hostname=$SYSTEM_NAME&uptime=$SYSTEM_UPTIME HTTP/1.0
    \r\n
    \r\n
    exit
```

send-schedule periodic <*value*>

Use the **send-schedule periodic** command to specify the amount of time (in milliseconds) between sending individual test packets during the probe. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the time interval between the individual packets. The valid range is **5** to **5000** milliseconds.

Default Values

By default, the time interval is **20** milliseconds.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example specifies a **45** millisecond time interval between the packets during **probe1** test:

(config)**#probe probe1 twamp**
(config-probe-probe1)**#send-schedule periodic 45**

size *<payload length>*

Use the **size** command to specify the length of the probe's test packet payload. Use the **no** form of this command to return to the default setting.

Syntax Description

<payload length>	Specifies size of test packet's payload. Valid range is **0** to **1462** bytes.

Default Values

By default, the payload length is **0** bytes.

Command History

Release 13.1	Command was introduced.
Release 17.2	Command was updated with a new default, range, and description.

Usage Examples

The following example sets the length of the Internet Control Message Protocol (ICMP) echo packet's padding field for **probe1** to **25** bytes:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#size 25**

source-address <*ip address*>

Use the **source-address** command to associate an IP address source for probe traffic. Use the **no** form of this command to remove the source IP address.

Syntax Description

<ip address>	Specifies a valid IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, the IP address of the outbound interface is used.

Command History

Release 13.1	Command was introduced.

Functional Notes

A valid local IP address must be entered for proper functionality.

Usage Examples

The following example configures the source IP address on **probe1**:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#source-address 10.10.10.1**

source-port <*port*>

Use the **source-port** command to specify a port source to use for probe traffic. Use the **no** form of this command to return to the default setting.

Syntax Description

<*port*>	Specifies the port number. Valid range is **0** to **65535**.

Default Values

By default, the port is set to **0** which means that the probe will dynamically select the port number.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example configures the source port on **probe1** as **5000**:

(config)**#probe probe1 http-request**
(config-probe-probe1)**#source-port 5000**

threshold

Use the **threshold** command to specify the criteria for a probe to be declared as passing or failing for the **delay**, **ipdv-abs**, and **packet-loss** values measured by the probe. Any combination of direction and type of threshold can be simultaneously configured and performed during the probe. Use the **no** form of this command to return to the default setting. Variations of this command include the following:

threshold delay [in | out | round-trip] [avg | max | min] *<fail value> <pass value>*
threshold ipdv-abs [in | out | round-trip] [avg | max | min] *<fail value> <pass value>*
threshold packet-loss round-trip [avg | max | min] *<fail value> <pass value>*

Syntax Description

delay	Specifies the thresholds for changing the state of the probe between pass and fail based on the measured delay. The fail and pass value range is **-2147483648** to **2147483647** milliseconds.
ipdv-abs	Specifies the thresholds for changing the state of the probe between pass and fail based on measured interpacket delay variation (IPDV). The fail and pass value range is **0** to **4294967295** milliseconds.
in	Specifies inbound delay or IPDV.
avg	Specifies the inbound average delay or IPDV.
max	Specifies the inbound maximum delay or IPDV.
min	Specifies the inbound minimum delay or IPDV.
out	Specifies outbound delay or IPDV.
avg	Specifies the outbound average delay or IPDV.
max	Specifies the outbound maximum delay or IPDV.
min	Specifies the outbound minimum delay or IPDV.
round-trip	Specifies round trip delay or IPDV.
packet-loss	Specifies the thresholds for changing the state of the probe between pass and fail based on measured packet loss. The fail and pass value range is **1** to **1000** packets.
round-trip	Specifies round trip packet loss.
avg	Specifies the average round trip packet loss.
max	Specifies the maximum round trip packet loss.
min	Specifies the minimum round trip packet loss.
<fail value>	Specifies the probe's failing value. Refer to the specific threshold type above for the valid range.
<pass value>	Specifies the probe's passing value. Refer to the specific threshold type above for the valid range.

Default Values

By default, the **delay** pass and fail value is **2147483647** milliseconds, the **ipdv-abs** pass and fail value is **4294967295** milliseconds, and the **packet-loss** pass and fail value is **1000**. This disables each of these thresholds by default.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example configures the probe to fail if it loses **100** packets and change to pass if packet loss is below **75**:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#threshold packet-loss in max 100 75**

timeout <*value*>

Use the **timeout** command to specify the amount of time to wait for a test result before determining a failure. Use the **no** form of this command to remove the timeout setting.

Syntax Description

<*value*>	Specifies the timeout value in milliseconds. This value must be less than the probe period value (refer to *dscp <value> on page 4071*). Valid range is **1** to **900000** milliseconds.

Default Values

By default, the timeout is **2000** milliseconds, and **10000** milliseconds (10 seconds) for Transmission Control Protocol (TCP) connect probes and **10000** milliseconds (10 seconds) for Hypertext Transfer Protocol (HTTP) request probes.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example configures AOS to wait **90** milliseconds before determining a failure on **probe1**:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#timeout 90**

tolerance

Use the **tolerance** command to configure the tolerance limit for test failures before returning a fail status from the probe. Limits can be specified for consecutive failures or by rate of failure. Tolerance levels can also be different based upon whether the probe is transitioning to the pass or fail state. Use the **no** form of this command to remove tolerance levels from probes. Variations of this command include:

tolerance consecutive fail <*number*>
tolerance consecutive pass <*number*>
tolerance consecutive fail <*number*> **pass** <*number*>
tolerance rate fail <*number*> **of** <*set size*>
tolerance rate pass <*number*> **of** <*set size*>
tolerance rate fail <*number*> **pass** <*number*> **of** <*set size*>

The probe is not operational until tolerance is defined.

Syntax Description

consecutive	Specifies that the probe state transitions occur only after a consecutive number of test results conflict with the current state.
rate	Specifies that the probe state transitions occur after a certain ratio of test results conflict with the current state.
fail <*number*>	Specifies the number of failures that must occur before transitioning the probe to the FAIL state. Valid ranges are **1** to **255** consecutive failures and **1** to **254** failures per set.
pass <*number*>	Specifies the number of passes before transitioning the probe to the PASS state. Valid ranges are **1** to **255** consecutive passes and **1** to **254** passes per set.
of <*set size*>	Specifies test set size for rate configuration. Valid range is **1** to **255**.

Default Values

By default, there are no configured tolerance levels. Therefore, a probe that does not have a defined tolerance will never fail.

When probes are set in **consecutive** mode, any state not explicitly configured has its tolerance value set to **1**.

In **rate** mode, any state not explicitly configured has its tolerance value set to 1+s-t, where ‘s’ is the set size and ‘t’ is the value of the other state.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command revised to include **pass** and **fail** values.
Release 17.2	Command was added to the Two-Way Active Measurement Protocol (TWAMP) and Internet Control Message Protocol (ICMP) timestamp probes.

Functional Notes

This command has been modified from its original form. All tolerance configurations before Revision 15.1 are deprecated, but will be supported for existing units that are upgraded.

Usage Examples

The following example configures probe1 to allow **10** consecutive failures before changing the probe status to FAIL, and requires **5** consecutive passes to change its status to PASS when in the FAIL state:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#tolerance consecutive fail 10 pass 5**

In the following example, the probe is configured for rate tolerance. To move to the FAIL state, 5 of the last 10 tests must fail. Once in this state, **8** of the last **10** tests must pass in order to transition the probe back to PASS:

(config)**#probe probe1 icmp-echo**
(config-probe-probe1)**#tolerance rate fail 5 pass 8 of 10**

type

Use the **type** command to specify a Hypertext Transfer Protocol (HTTP) request type. Use the **no** form of this command to return to the default setting. Variations of this command include:

type get
type head
type raw

Syntax Description

get	Specifies the probe to use HTTP **get** request.
head	Specifies the probe to use HTTP **head** request.
raw	Specifies the probe to use HTTP **raw** request.

Default Values

By default, the probe's HTTP request is set to **get**.

Command History

Release 13.1	Command was introduced.

Functional Notes

This command can only be executed while in the **probe** <*name*> **http-request** command set.

Usage Examples

The following example configures **probe1** to use HTTP request **raw**:

(config)**#probe probe1 http-request**
(config-probe-probe1)**#type raw**

vrf *<name>*

Use the **vrf** command to specify the virtual routing and forwarding (VRF) instance in which the probe operates. Use the **no** form of this command to associate the probe with the default (unnamed) VRF.

Syntax Description

<name>	Specifies the name of the VRF instance. If no VRF is specified, the probe operates within the default (unnamed) VRF instance.

Default Values

By default, probes operate within the default (unnamed) VRF instance.

Command History

Release 17.1	Command was introduced.
Release 18.3	Command was added to Border Gateway Protocol (BGP) and Dynamic Host Control Protocol (DHCP) version 4 (DHCPv4) and version 6 (DHCPv6).
Release R11.2.0	Command was added to network monitoring.

Usage Examples

The following example specifies that the VRF instance **RED** is used for **probe1**:

(config)**#probe probe1 http-request**
(config-probe-probe1)**#vrf RED**

NETWORK MONITOR PROBE RESPONDER COMMAND SET

This section explains the commands available for Network Monitoring Probe Responders. A probe responder is the general term used for a variety of server applications that respond to the network monitor probe types. The Two-Way Active Measurement Protocol (TWAMP) probe responder encompasses the responder side of the TWAMP-Control protocol by responding to TWAMP-Control messages and acting as a remote endpoint for test packets. The Internet Control Message Protocol (ICMP) timestamp probe responder responds to ICMP timestamp request packets so that it can act as a remote endpoint for ICMP timestamp probes. Commands common to all the probe responder types are identified in the following section, as well as isolated commands that only apply to the specific probe responder types.

To activate the Network Monitor Probe Responder Configuration mode, enter the **probe responder** command at the Global Configuration mode prompt followed by the probe type. Specify the probe responder type of **icmp-timestamp**, **twamp**, and **udp-echo**. For example:

```
>enable
#configure terminal
(config)#probe responder twamp
(config-responder-twamp)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
cross-connect on page 76 (applicable to the ICMP timestamp and UDP echo responders only)
exit on page 83
interface on page 84
shutdown on page 93

The following commands are applicable to ICMP timestamp probe responder types and can be executed after this command:

(config)**#probe responder icmp-timestamp**

access-class <name> in on page 4091

The following commands are applicable to TWAMP probe responder types and can be executed after this command:

(config)**#probe responder twamp**

access-class <name> in on page 4091
control source-port on page 4092
control timeout <value> on page 4093
max-sessions <value> on page 4094
port <value> on page 4095

source-interface <interface> on page 4096
test timeout <value> on page 4097

The following commands are applicable to User Datagram Protocol (UDP) echo probe responder types and can be executed after this command:

(config)**#probe responder udp-echo**

access-class <name> in on page 4091
port <value> on page 4095
source-interface <interface> on page 4096

access-class <*name*> in

Use the **access-class in** command to specify an access control list (ACL) to filter access to the responder. Use the **no** form of this command to remove the ACL from the responder. Variations of this command include:

access-class <*name*> **in**
access-class <*name*> **in any-vrf**
access-class <*name*> **in vrf** <*name*>

Syntax Description

access-class <*name*>	Specifies a name of the ACL.
any-vrf	Optional. Specifies that the ACL used by the responder can be located in any virtual routing and forwarding (VRF) instance.
vrf <*name*>	Optional. Specifies a VRF instance in which the ACL used by the responder resides. If no VRF is specified, the default (unnamed) VRF is used.

Default Values

By default, no ACL is configured.

Command History

Release 17.2	Command was introduced.
Release R11.2.0	Command was expanded to include the **any-vrf** and **vrf** <*name*> parameters.

Usage Examples

The following example sets an ACL for the Two-Way Active Measurement Protocol (TWAMP) responder:

(config)**#probe responder twamp**
(config-responder-twamp)**#access-class Anet in**

control source-port

Use the **control source-port** command to specify the Two-Way Active Measurement Protocol (TWAMP) source control port. Use the **no** form of this command to return to the default setting. Variations of this command include:

control source-port owamp-control
control source-port twamp-control
control source-port <*port*>

Syntax Description

owamp-control	Specifies One-Way Active Measurement Protocol (OWAMP) control port (861) as the source port.
twamp-control	Specifies the default TWAMP control port (862) as the source port.
<*port*>	Specifies a source TWAMP control port other than the default port 862. The valid range is **1** to **65535**.

Default Values

By default, the source port is the TWAMP control port, port **862**.

Command History

Release 17.2	Command was introduced.
Release 17.6	Command was expanded to include the **twamp-control** parameter and the default source port was set to port **862**.

Usage Examples

The following example specifies the OWAMP control port as the source control port for the TWAMP responder:

(config)**#probe responder twamp**
(config-responder-twamp)**#control source-port owamp-control**

control timeout <*value*>

Use the **control timeout** command to set the Two-Way Active Measurement Protocol (TWAMP) control session timeout value. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the timeout interval in seconds. Range is **1** to **65535**.

Default Values

By default, the control timeout value is set to **900**.

Command History

Release 17.6	Command was introduced.

Usage Examples

In the following example, the TWAMP control session is set to timeout after **7200** seconds:

(config)**#probe responder twamp**
(config-responder-twamp)**#control timeout 7200**

max-sessions *<value>*

Use the **max-sessions** command to specify the number of simultaneous Two-Way Active Measurement Protocol (TWAMP) control sessions the responder can handle. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the maximum number of simultaneous TWAMP-control sessions.

Default Values

By default, the maximum sessions is **10**.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example specifies the **max-sessions** value of **5**:

(config)**#probe responder twamp**
(config-responder-twamp)**#max-sessions 5**

port *<value>*

Use the **port** command to specify the User Datagram Protocol (UDP) port to listen for and respond to UDP echo packets. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the port number. Valid range is **1** to **65535**.

Default Values

By default, the UDP port value is **6**.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example specifies **port 5055** as the UDP port for the UDP echo responder:

(config)**#probe responder udp-echo**
(config-responder-udp)**#port 5055**

source-interface <*interface*>

Use the **source-interface** command to specify an interface with the primary IP address used as the source address for responder traffic that originated from the unit. Use the **no** form of this command to return to the default setting. Variations of this command include:

source-interface <*interface*>
vrf <*name*> **source-interface** <*interface*>

Syntax Description

<*interface*>	Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**.
vrf <*name*>	Optional. Specifies a virtual routing and forwarding (VRF) instance in which the source interface resides. If no VRF is specified, the default (unnamed) VRF is used.

Default Values

By default, the source interface is not configured.

Command History

Release 17.2	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release R11.2.0	Command was expanded to include the **vrf** parameter.

Usage Examples

The following example configures the source interface as **vlan1**:

(config)**#probe responder twamp**
(config-responder-twamp)#source-interface **vlan1**

test timeout *<value>*

Use the **test timeout** command to set the timeout value associated with the Two-Way Active Management Protocol (TWAMP) probe responder test session. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the timeout interval in seconds. Range is **1** to **65535**.

Default Values

By default, the test session timeout is set to **900** seconds.

Command History

Release 17.6	Command was introduced.

Usage Examples

The following example sets the TWAMP probe responder's timeout interval to **7200** seconds:

(config)**#probe responder twamp**
(config-responder-twamp)**#test timeout 7200**

NETWORK MONITOR TRACK COMMAND SET

This section explains the commands available for Network Monitoring Tracks. Tracks are objects created to monitor network probes for a change in their state. The tracks can be configured to perform a specific action based upon the probe state detected. Association between a track and a probe occurs through referencing the probe in the track's configuration. Once the track is registered with the probe, whenever a change occurs with the probe's state, an event is sent to the track.

Additional configuration commands are available for creating probes. These are explained in the *Network Monitor Probe Command Set on page 4062*.

To activate the Network Monitor Track Configuration mode, enter the **track** command at the Global Configuration mode prompt followed by the name of the track. For example:

```
>enable
#configure terminal
(config)#track track1
(config-track)#
```

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

dampening-interval on page 4099
log-changes on page 4100
snmp trap state-change on page 4101
test if on page 4102
test list on page 4108
test list weighted on page 4113
time-schedule <name> on page 4118

dampening-interval

Use the **dampening-interval** command to specify an amount of time to wait before allowing a new probe status change to trigger a new action. Use the **no** form of this command to return to the default setting. Variations of this command include:

dampening-interval <*value*>
dampening-interval fail<*value*>
dampening-interval pass <*value*>

Syntax Description

<*value*>	Specifies the time interval value in seconds. Valid range is **1** to **4294967295** seconds. If neither the **fail** or **pass** subcommand is specified, the value will be used for both conditions.
fail <*value*>	Specifies the delay in seconds following pass-to-fail transitions before a new action can be triggered.
pass <*value*>	Specifies the delay in seconds following fail-to-pass transitions before a new action can be triggered.

Default Values

By default, the interval is set to **1** seconds.

Command History

Release 13.1	Command was introduced.
Release 14.1	Command was expanded to include the **fail** and **pass** criteria.

Usage Examples

The following example sets the dampening interval to **90** seconds for a fail-to-pass transition:

(config)**#track track1**
(config-track)**#dampening-interval pass 90**

log-changes

Use the **log-changes** command to enable logging of status changes. When enabled, probe state transitions are displayed (real time) on the terminal (or Telnet) screen. Unlike **track debug** commands, the **log-changes** command appears in the running configuration and can be saved to persist through a unit restart. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example enables the logging of status changes:

```
(config)#track track1
(config-track)#log-changes
```

snmp trap state-change

Use the **snmp trap state-change** command to enable the network monitor track to send a Simple Network Management Protocol (SNMP) trap when a change in state occurs. Use the **no** form of this command to disable the trap.

Syntax Description

No subcommands.

Default Values

By default, the state-change trap is disabled.

Command History

Release 18.1	Command was introduced.

Functional Notes

The network monitor track set of traps must also be enabled using the **snmp-server enable traps track** command in the Global Configuration mode. Refer to *snmp-server enable traps on page 1792* for more information.

Additional configuration steps are necessary to configure SNMP traps for this feature to function. Refer to the *SNMP in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables the **snmp trap state-change** for network monitoring:

```
(config)#track track1
(config-track)#snmp trap state-change
```


test if

Use the **test if** command to specify a single object (schedule, probe, or interface) to be tested. Use the **no** form of this command to remove the track test. Variations of this command include:

test if ethernet y1731 meg char-string <*name*> <*level*> <*id*> **loc**
test if ethernet y1731 meg char-string <*name*> <*level*> <*id*> **rdi**
test if ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **loc**
test if ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **rdi**
test if interface <*interface*> **downspeed** <*speed*>
test if interface <*interface*> **ip-routing**
test if interface <*interface*> **ipv6-routing**
test if interface <*interface*> **line-protocol**
test if interface <*interface*> **upspeed** <*speed*>
test if interface system-control-evc downspeed <*speed*>
test if interface system-control-evc ip-routing
test if interface system-control-evc ipv6-routing
test if interface system-control-evc line-protocol
test if interface system-control-evc upspeed <*speed*>
test if interface system-management-evc ip-routing
test if interface system-management-evc ipv6-routing
test if interface system-management-evc line-protocol
test if ip ffe entries less-than <*number*>
test if ip ffe <*ingress interface*> **entries less-than** <*number*>
test if ipv6 ffe entries less-than <*number*>
test if ipv6 ffe <*ingress interface*> **entries less-than** <*number*>
test if probe <*name*>
test if schedule <*name*>
test if voice user <*extension*> **registered**

test if not ethernet y1731 meg char-string <*name*> <*level*> <*id*> **loc**
test if not ethernet y1731 meg char-string <*name*> <*level*> <*id*> **rdi**
test if not ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **loc**
test if not ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **rdi**
test if not interface <*interface*> **downspeed** <*speed*>
test if not interface <*interface*> **ip-routing**
test if not interface <*interface*> **ipv6-routing**
test if not interface <*interface*> **line-protocol**
test if not interface <*interface*> **upspeed** <*speed*>
test if not interface system-control-evc downspeed <*speed*>
test if not interface system-control-evc ip-routing
test if not interface system-control-evc ipv6-routing
test if not interface system-control-evc line-protocol
test if not interface system-control-evc upspeed <*speed*>
test if not interface system-management-evc ip-routing
test if not interface system-management-evc ipv6-routing

test if not interface system-management-evc line-protocol
test if not ip ffe entries less-than <*number*>
test if not ip ffe <*ingress interface*> **entries less-than** <*number*>
test if not ipv6 ffe entries less-than <*number*>
test if not ipv6 ffe <*ingress interface*> **entries less-than** <*number*>
test if not probe <*name*>
test if not schedule <*name*>
test if not voice user <*extension*> **registered**

Syntax Description

ethernet y1731 meg	Specifies a Y.1731 maintenance endpoint (MEP) as the object to be tested.
char-string <*name*>	Specifies a Y.1731 maintenance entity group (MEG) name using a character string format. Maximum length is **45** ASCII characters.
icc-umc <*name*>	Specifies a Y.1731 MEG name using the ITU-CarrierCode Unique MEG ID Code MEG (ICC-UMC) format. Maximum length is **13** ASCII characters.
<*level*>	Specifies the MEG level. Valid range is **0** to **7**.
<id>	Specifies the MEP ID. Valid range is **1** to **8191**.
loc	Specifies that the track will inspect the specified MEP for indication of loss of continuity (LOC). The test will report TRUE if the specified MEP reports an LOC condition.
rdi	Specifies that the track will inspect the specified MEP for remote defect indication (RDI). The test will report TRUE if the specified MEP reports an RDI condition.
interface <*interface*>	Specifies an interface as the object to be tested. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network interface, use **vlan 1**. Type **test if interface ?** for a complete list of valid interfaces.
downspeed <*speed*>	Specifies the downstream speed (in kilobits per second) will be tested. The downstream speed is the receive speed of an interface from the perspective of the unit. The test will report TRUE if the interface downstream speed is greater than or equal to the specified downstream speed.
ip-routing	Specifies the interface's ability to perform Internet Protocol version 4 (IPv4) routing will be tested.
ipv6-routing	Specifies the interface's ability to perform Internet Protocol version 6 (IPv6) routing will be tested.
line-protocol	Specifies the line-protocol state of an interface will be tested.

upspeed <*speed*>	Specifies the upstream speed (in kilobits per second) will be tested. The upstream speed is the transmit speed of an interface from the perspective of the unit. The test will report TRUE if the interface upstream speed is greater than or equal to the specified downstream speed.
interface system-control-evc	Specifies the system control Ethernet virtual connection (EVC) is the object to be tested.
interface system-management-evc	Specifies the system management EVC is the object to be tested.
ip ffe entries less-than	Tests that the number of RapidRoute flow entries is less than the specified number for IPv4.
ipv6 ffe entries less-than	Tests that the number of RapidRoute flow entries is less than the specified number for IPv6.
<*number*>	The specified maximum number of RapidRoute flow entries for the test. Valid range is **1** to **500000** entries.
<*ingress interface*>	Optional. Specifies that only a single ingress interface is tested for RapidRoute entries. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network interface, use **vlan 1**. Type **test if ip ffe ?** for a complete list of valid interfaces.
not	Optional. Negates the test results when specifying a single object (schedule, probe, or interface) to be tested.
probe <*name*>	Specifies the name of the probe.
schedule <*name*>	Specifies the name of the schedule.
voice user <*extension*> **registered**	Tests the SIP registration status of the specified voice user.

Network monitoring probes and their associated names are created using the command *probe on page 1666**. Schedules and their associated names are created using the command* *schedule <name> on page 1695**. For more information about interfaces, refer to the command* *interface on page 84**.*

Default Values

By default, a track is not associated with any probes or interfaces.

Functional Notes

The **test if** command specifies a conditional test where the track state (pass or fail) is dependent upon the state of the object (probe, schedule, or interface) being tested. For example, the track will PASS if the schedule or probe is in an ACTIVE or PASS state. Conversely, the track will FAIL if the schedule or probe is in an INACTIVE or FAIL state.

The **test if not** command specifies a conditional test where the track state (pass or fail) is dependent upon the state of the object (probe, schedule, or interface) being tested. The **not** keyword indicates that the track state will negate the result of the object test. For example, the track will FAIL if the schedule or probe is in an ACTIVE or PASS state. Conversely, the track will PASS if the schedule or probe is in an INACTIVE or FAIL state.

An interface is IP routing if its line-protocol state is up and if it has a valid, nonzero IP address. This means that interfaces using Dynamic Host Configuration Protocol (DHCP) or negotiated Point-to-Point Protocol (PPP) will not pass until their primary IP address is dynamically configured.

Command History

Release 15.1	Command was introduced.
Release 16.1	Command was expanded to include the **interface** parameter.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release R10.7.0	Command was expanded to include the **ipv6-routing** parameter.
Release R10.10.0	Command was expanded to include the system control EVC.
Release R10.11.0	Command was expanded to include the **ethernet y1731 meg**, **downspeed**, and **upspeed** parameters, as well as the Ethernet in the first mile (EFM) group interface.
Release R11.2.0	Command was expanded to include the High-level Data Link Control (HDLC) interface.
Release R11.5.0	Command was expanded to include the switchport interface, Gigabit Ethernet switchport interface, and 10-Gigabit Ethernet switchport interface.
Release R11.10.0	Command was expanded to include the **ip ffe entries less-than**, **ipv6 ffe entries less-than** and **voice user** <*extension*> **registered** parameters.

Usage Examples

The following example demonstrates the use of the **test if probe** command to specify a single object to test:

(config)**#track PINGTEST**
(config-track)**#test if probe PINGREMOTE**

The following example demonstrates the logic of the **test if not** command used with schedule tracking:

(config)**#track DELAY**
(config-track)**#test if not schedule DELAY-AFTER-BOOT**

The inverse logic of this command means that track DELAY will pass only if the schedule DELAY-AFTER-BOOT is inactive.

The explanation that follows uses a real-world example to provide insight into the example above:

A customer has a primary Ethernet wide area network (WAN) interface, as well as a dial-on-demand interface enabled on an AOS unit. The demand interface is intended as a backup for the primary Ethernet interface. During router initialization and bootup, the Ethernet interface negotiates an IPv4 address and default route from a DHCP server. Due to this negotiation process, the active state of the Ethernet interface lags behind that of the demand interface. As a result, the Ethernet interface appears down and the demand interface dials out to back up the connection. The customer would like to prevent the demand interface from dialing out before the Ethernet connection has had a chance to obtain its DHCP settings and become active. It is determined that 180 seconds is a sufficient amount of time to allow for the Ethernet interface to become active.

The following bullets describe the setup via command line interface (CLI) to accomplish the customer's goals:

- A schedule called DELAY-AFTER-BOOT is created and specified to become active 180 seconds after the AOS unit has booted up.
- A track named DELAY is created.
- Track DELAY is associated with the schedule DELAY-AFTER-BOOT via the following command:

  (config-track-DELAY)**#test if not schedule DELAY-AFTER-BOOT**

  The inverse logic of this command means that track DELAY will pass only if the schedule DELAY-AFTER-BOOT is inactive. Therefore, this track will pass only during the first 180 seconds following bootup of the AOS unit.
- A default route to null interface 0 is created and associated with track DELAY. This default route will only be inserted into the routing table when track DELAY is in the pass state. The administrative distance for the default route to null interface 0 is 10 and is set to be lower than the administrative distance for the demand interface default route (200).

Output from the **show run** command summarizes the CLI configuration:

```
#show run
(some output omitted)…
.schedule DELAY-AFTER-BOOT
!! Schedule is Inactive for first 180 seconds, then Active thereafter
 relative start-after 180
!
track DELAY
 log-changes
 test if not schedule DELAY-AFTER-BOOT
 no shutdown
!
!!! Below is a default route to null 0 with an admin distance of
!!! 10 that is tracked by DELAY and a default route to demand 1
!!! with admin distance of 200
ip route 0.0.0.0 0.0.0.0 null 0 10 track DELAY
ip route 0.0.0.0 0.0.0.0 demand 1 200
```


Since track DELAY is in a pass state during the first 180 seconds after the AOS unit has booted up, the default route to null interface 0 will be in effect and all traffic using the default route in the route table will be routed to null interface 0. The demand interface will not be activated during the first 180 seconds because the default route to null interface 0 has a lower administrative distance than the demand interface default route.

As soon as a default route has been assigned to the primary Ethernet WAN interface, the route will appear in the routing table with an administrative distance of 1 (which is lower than the administrative distance of 10 for the null interface). Due to the lower administrative distance, all traffic using the default route in the route table will switch to the default route associated with the primary Ethernet interface.

180 seconds after bootup, the schedule DELAY-AFTER-BOOT becomes active. Subsequently, track DELAY fails. The default route to null interface 0 is removed from the routing table and will not be placed in the route table again as long as the AOS unit is up. The two default routes that remain are the current default route to the primary WAN Ethernet interface (administrative distance is 1) and the backup default route to the demand interface (administrative distance is 200).

The following example uses the **test if interface** command to specify testing the IPv4 routing capability of an Ethernet interface:

```
(config)#track track1
(config-track-track1)#test if interface ethernet 0/1 ip-routing
```

To view the results of the test, use the **do show track track1** command:

```
(config-track-track1)#do show track track1
 Current State: FAIL     (Admin: UP)
 Testing:
   interface eth 0/1 ip-routing (FAIL)
 Dampening Interval: 1 seconds
 Time in current state: 0 days, 0 hours, 0 minutes, 4 seconds
 Track State Changes: 1
 Tracking:
```


test list

Use the **test list** command to enter the Boolean Track Test List command set, which is used to specify multiple objects (schedules, probes, or interfaces) to be tested. Use the **no** form of this command to remove the test list. Variations of this command include:

test list and
test list or

The following additional subcommands are available once you have entered the Boolean Track Test List Configuration mode:

if ethernet y1731 meg char-string <*name*> <*level*> <*id*> **loc**
if ethernet y1731 meg char-string <*name*> <*level*> <*id*> **rdi**
if ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **loc**
if ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **rdi**
if interface <*interface*> **downspeed** <*speed*>
if interface <*interface*> **ip-routing**
if interface <*interface*> **ipv6-routing**
if interface <*interface*> **line-protocol**
if interface <*interface*> **upspeed** <*speed*>
if interface system-control-evc downspeed <*speed*>
if interface system-control-evc ip-routing
if interface system-control-evc ipv6-routing
if interface system-control-evc line-protocol
if interface system-control-evc upspeed <*speed*>
if interface system-management-evc ip-routing
if interface system-management-evc ipv6-routing
if interface system-management-evc line-protocol
if ip ffe entries less-than <*number*>
if ip ffe <*ingress interface*> **entries less-than** <*number*>
if ipv6 ffe entries less-than <*number*>
if ipv6 ffe <*ingress interface*> **entries less-than** <*number*>
if probe <*name*>
if schedule <*name*>
if voice user <*extension*> **registered**

if not ethernet y1731 meg char-string <*name*> <*level*> <*id*> **loc**
if not ethernet y1731 meg char-string <*name*> <*level*> <*id*> **rdi**
if not ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **loc**
if not ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **rdi**
if not interface <*interface*> **downspeed** <*speed*>
if not interface <*interface*> **ip-routing**
if not interface <*interface*> **ipv6-routing**
if not interface <*interface*> **line-protocol**
if not interface <*interface*> **upspeed** <*speed*>
if not interface system-control-evc downspeed <*speed*>

if not interface system-control-evc ip-routing
if not interface system-control-evc ipv6-routing
if not interface system-control-evc line-protocol
if not interface system-control-evc upspeed <*speed*>
if not interface system-management-evc ip-routing
if not interface system-management-evc ipv6-routing
if not interface system-management-evc line-protocol
if not ip ffe entries less-than <*number*>
if not ip ffe <*ingress interface*> **entries less-than** <*number*>
if not ipv6 ffe entries less-than <*number*>
if not ipv6 ffe <*ingress interface*> **entries less-than** <*number*>
if not probe <*name*>
if not schedule <*name*>
if not voice user <*extension*> **registered**

When using any command under the Boolean AND/OR track test list, it is important to remember how the logic will affect every object in the track test list.

Syntax Description

and	Specifies the relationship between all objects placed in this list. The logical AND relationship means that all objects in this list must be in the PASS state for the track test list to pass, or at least one object must be in a FAIL state for the track test list to fail.
or	Specifies the relationship between all objects placed in this list. The logical OR relationship means that only one of the objects in this list must be in the PASS state for the track test list to pass, and all objects in a FAIL state for the track test list to fail.
if	Specifies a single conditional test to be added to the test track list.
if not	Specifies a single conditional test to be added to the test track list. The **not** keyword indicates that the individual track state will negate the result of the object test.
ethernet y1731 meg	Specifies a Y.1731 maintenance endpoint (MEP) as the object to be tested.
char-string <*name*>	Specifies a Y.1731 maintenance entity group (MEG) name using a character string format. Maximum length is **45** ASCII characters.
icc-umc <*name*>	Specifies a Y.1731 MEG name using the ITU-CarrierCode Unique MEG ID Code MEG (ICC-UMC) format. Maximum length is **13** ASCII characters.
<*level*>	Specifies the MEG level. Valid range is **0** to **7**.
<id>	Specifies the MEP ID. Valid range is **1** to **8191**.

loc	Specifies that the track will inspect the specified MEP for indication of loss of continuity (LOC). The test will report TRUE if the specified MEP reports an LOC condition.
rdi	Specifies that the track will inspect the specified MEP for remote defect indication (RDI). The test will report TRUE if the specified MEP reports an RDI condition.
interface <*interface*>	Specifes an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network interface, use **vlan 1**. Type **if interface ?** for a complete list of valid interfaces.
downspeed <*speed*>	Specifies the downstream speed (in kilobits per second) will be tested. The downstream speed is the receive speed of an interface from the perspective of the unit. The test will report TRUE if the interface downstream speed is greater than or equal to the specified downstream speed.
ip-routing	Specifies the interface's ability to perform Internet Protocol version 4 (IPv4) routing will be tested.
ipv6-routing	Specifies the interface's ability to perform Internet Protocol version 6 (IPv6) routing will be tested.
line-protocol	Specifies the line-protocol state of an interface will be tested.
upspeed <*speed*>	Specifies the upstream speed (in kilobits per second) will be tested. The upstream speed is the transmit speed of an interface from the perspective of the unit. The test will report TRUE if the interface upstream speed is greater than or equal to the specified downstream speed.
interface system-control-evc	Specifies the system control Ethernet virtual connection (EVC) is added to the test track list.
interface system-management-evc	Specifies the system management EVC is added to the test track list.
ip ffe entries less-than	Tests that the number of RapidRoute flow entries is less than the specified number for IPv4.
ipv6 ffe entries less-than	Tests that the number of RapidRoute flow entries is less than the specified number for IPv6.
<*number*>	The specified maximum number of RapidRoute flow entries for the test. Valid range is **1** to **500000** entries.
<*ingress interface*>	Optional. Specifies that only a single ingress interface is tested for RapidRoute entries. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network interface, use **vlan 1**. Type **if ip ffe ?** for a complete list of valid interfaces.

probe <*name*>	Specifies the name of the probe.
schedule <*name*>	Specifies the name of the schedule.
voice user <*extension*> **registered**	Tests the SIP registration status of the specified voice user.

Network monitoring probes and their associated names are created using the command *probe on page 1666**. Schedules and their associated names are created using the command* *schedule <name> on page 1695**. For more information about interfaces, refer to the command* *interface on page 84**.*

Default Values

By default, a track list does not exist.

Command History

Release 15.1	Command was introduced.
Release 16.1	Command was expanded to include the **interface** parameter.
Release R10.7.0	Command was expanded to include the **ipv6-routing** parameter.
Release R10.10.0	Command was expanded to include the system control EVC.
Release R10.11.0	Command was expanded to include the **ethernet y1731 meg**, **downspeed**, and **upspeed** parameters, as well as the Ethernet in the first mile (EFM) group interface.
Release R11.2.0	Command was expanded to include the High-level Data Link Control (HDLC) interface.
Release R11.5.0	Command was expanded to include the switchport interface, Gigabit Ethernet switchport interface, and 10-Gigabit Ethernet switchport interface.
Release R11.10.0	Command was expanded to include the **ip ffe entries less-than**, **ipv6 ffe entries less-than** and **voice user** <*extension*> **registered** parameters.

Functional Notes

There is no limit to how many probes, schedules, or interfaces can be tested within a single test list. However, only one type (AND, OR, or weighted) of test list can exist on a track at any given time.

An interface is IPv4 routing if its line-protocol state is up and if it has a valid, nonzero IPv4 address. This means that interfaces using Dynamic Host Configuration Protocol (DHCP) or negotiated Point-to-Point Protocol (PPP) will not pass until their primary IPv4 address is dynamically configured.

Usage Examples

The following example demonstrates use of the **test list and** command to create a Boolean track test list where ALL tests must PASS in order for the track to PASS. The test list for track LB contains two probe tests, LB and LB2.

(config)**#track LB**
(config-track)**#test list and**
(config-track-test)**#if probe LB**
(config-track-test)**#if probe LB2**
(config-track-test)**#exit**
(config-track)**#no shutdown**

The **show track LB** command is executed to see whether track LB is in a PASS state:

#show track LB
Current State: PASS (Admin: UP)
Testing:
probe LB (PASS)
AND probe LB2 (PASS)
Dampening Interval: 1 seconds
Time in current state: 0 days, 0 hours, 0 minutes, 29 seconds
Track State Changes: 2
Tracking:

Currently, track LB is in a PASS state. Due to the AND Boolean logic for this test list, track LB is in a PASS state because the test probe statements within the test list (probe LB and LB2) are also BOTH in a PASS state.

Now, probe LB has been forced to fail for demonstration purposes in this example. Output from the **show track LB** command shows track LB in a FAIL state.

(config-loop 1)**#do show track LB**

Current State: FAIL (Admin: UP)
Testing:
probe LB (FAIL)
AND probe LB2 (PASS)
Dampening Interval: 1 seconds
Time in current state: 0 days, 0 hours, 0 minutes, 10 seconds
Track State Changes: 3
Tracking:

Probe LB is now in a FAIL state. As a result, track LB is also in a FAIL state.

*If the test list in this example had specified the OR Boolean logic (using the **test list or** command), then track LB would have passed even though one of the test probes was in the FAIL state.*

test list weighted

Use the **test list weighted** command to enter the Weighted Track Test List Configuration mode, which is used to specify multiple objects (schedules, probes, or interfaces) to be tested. Objects listed in a weighted track test are assigned a specific weight value. The total weight of all the objects in the list is compared to a user-specified threshold to determine whether the track passes or fails. Use the **no** form of this command to remove the test list.

The following additional subcommands are available once you have entered the Weighted Track Test List Configuration mode:

if ethernet y1731 meg char-string <*name*> <*level*> <*id*> **loc weight** <*value*>
if ethernet y1731 meg char-string <*name*> <*level*> <*id*> **rdi weight** <*value*>
if ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **loc weight** <*value*>
if ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **rdi weight** <*value*>
if interface <*interface*> **downspeed** <*speed*> **weight** <*value*>
if interface <*interface*> **ip-routing weight** <*value*>
if interface <*interface*> **ipv6-routing weight** <*value*>
if interface <*interface*> **line-protocol weight** <*value*>
if interface <*interface*> **upspeed** <*speed*> **weight** <*value*>
if interface system-control-evc downspeed <*speed*> **weight** <*value*>
if interface system-control-evc ip-routing weight <*value*>
if interface system-control-evc ipv6-routing weight <*value*>
if interface system-control-evc line-protocol weight <*value*>
if interface system-control-evc upspeed <*speed*> **weight** <*value*>
if ip ffe entries less-than <*number*> **weight** <*value*>
if ip ffe <*ingress interface*> **entries less-than** <*number*> **weight** <*value*>
if ipv6 ffe entries less-than <*number*> **weight** <*value*>
if ipv6 ffe <*ingress interface*> **entries less-than** <*number*> **weight** <*value*>
if probe <*name*> **weight** <*value*>
if schedule <*name*> **weight** <*value*>

if voice user <*extension*> **registered weight** <*value*>
if not ethernet y1731 meg char-string <*name*> <*level*> <*id*> **loc weight** <*value*>
if not ethernet y1731 meg char-string <*name*> <*level*> <*id*> **rdi weight** <*value*>
if not ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **loc weight** <*value*>
if not ethernet y1731 meg icc-umc <*name*> <*level*> <*id*> **rdi weight** <*value*>
if not interface <*interface*> **downspeed** <*speed*> **weight** <*value*>
if not interface <*interface*> **ip-routing weight** <*value*>
if not interface <*interface*> **ipv6-routing weight** <*value*>
if not interface <*interface*> **line-protocol weight** <*value*>
if not interface <*interface*> **upspeed** <*speed*> **weight** <*value*>
if not interface system-control-evc downspeed <*speed*> **weight** <*value*>
if not interface system-control-evc ip-routing weight <*value*>
if not interface system-control-evc ipv6-routing weight <*value*>
if not interface system-control-evc line-protocol weight <*value*>
if not interface system-control-evc upspeed <*speed*> **weight** <*value*>

if not ip ffe entries less-than <*number*> **weight** <*value*>
if not ip ffe <*ingress interface*> **entries less-than** <*number*> **weight** <*value*>
if not ipv6 ffe entries less-than <*number*> **weight** <*value*>
if not ipv6 ffe <*ingress interface*> **entries less-than** <*number*> **weight** <*value*>
if not probe <*name*> **weight** <*value*>
if not schedule <*name*> **weight** <*value*>
if not voice user <*extension*> **registered weight** <*value*>
threshold <*number*>
threshold pass <*number*> **fail** <*number*>

Syntax Description

if	Specifies a single conditional test to be added to the test track list.
if not	Specifies a single conditional test to be added to the test track list. The **not** keyword indicates that the individual track state will negate the result of the object test.
ethernet y1731 meg	Specifies a Y.1731 maintenance endpoint (MEP) as the object to be tested.
char-string <*name*>	Specifies a Y.1731 maintenance entity group (MEG) name using a character string format. Maximum length is **45** ASCII characters.
icc-umc <*name*>	Specifies a Y.1731 MEG name using the ITU-CarrierCode Unique MEG ID Code MEG (ICC-UMC) format. Maximum length is **13** ASCII characters.
<*level*>	Specifies the MEG level. Valid range is **0** to **7**.
<id>	Specifies the MEP ID. Valid range is **1** to **8191**.
loc	Specifies that the track will inspect the specified MEP for indication of loss of continuity (LOC). The test will report TRUE if the specified MEP reports an LOC condition.
rdi	Specifies that the track will inspect the specified MEP for remote defect indication (RDI). The test will report TRUE if the specified MEP reports an RDI condition.
interface <*interface*>	Specifies an interface to add to the track test list. Specify interfaces in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network interface, use **vlan 1**. Type **if interface ?** for a complete list of valid interfaces.
downspeed <*speed*>	Specifies the downstream speed (in kilobits per second) will be tested. The downstream speed is the receive speed of an interface from the perspective of the unit. The test will report TRUE if the interface downstream speed is greater than or equal to the specified downstream speed.
ip-routing	Specifies the interface's ability to perform Internet Protocol version 4 (IPv4) routing will be tested.

ipv6-routing	Specifies the interface's ability to perform Internet Protocol version 6 (IPv6) routing will be tested.
line-protocol	Specifies the line-protocol state of an interface will be tested.
upspeed <*speed*>	Specifies the upstream speed (in kilobits per second) will be tested. The upstream speed is the transmit speed of an interface from the perspective of the unit. The test will report TRUE if the interface upstream speed is greater than or equal to the specified downstream speed.
interface system-control-evc	Specifies the system control Ethernet virtual connection (EVC) is added to the test track list.
ip ffe entries less-than	Tests that the number of RapidRoute flow entries is less than the specified number for IPv4.
ipv6 ffe entries less-than	Tests that the number of RapidRoute flow entries is less than the specified number for IPv6.
<*number*>	The specified maximum number of RapidRoute flow entries for the test. Valid range is **1** to **500000** entries.
<*ingress interface*>	Optional. Specifies that only a single ingress interface is tested for RapidRoute entries. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a virtual local area network interface, use **vlan 1**. Type **if ip ffe ?** for a complete list of valid interfaces.
probe <*name*>	Specifies the name of the probe or schedule.
schedule <*name*>	Specifies the name of the schedule.
threshold <*number*>	Specifies a baseline weight for state transitions. Range is **1** to **4294967295**.
fail <*number*>	Optional. Specifies the number that will change the state of the track test list to fail. Range is **1** to **4294967295**.
pass <*number*>	Optional. Specifies the number which, if reached or exceeded, will change the state of the track test list to pass. Range is **1** to **4294967295**.
voice user <*extension*> **registered**	Tests the SIP registration status of the specified voice user
weight <*value*>	Specifies the weight value to use if this test is successful. Range is **1** to **65535**.

Network monitoring probes and their associated names are created using the command *probe on page 1666**. Schedules and their associated names are created using the command* *schedule <name> on page 1695**. For more information about interfaces, refer to the command* *interface on page 84**.*

Default Values

By default, a track list does not exist.

Command History

Release 15.1	Command was introduced.
Release 16.1	Command was expanded to include the **interface** parameter.
Release R10.7.0	Command was expanded to include the **ipv6-routing** parameter.
Release R10.10.0	Command was expanded to include the system control EVC.
Release R10.11.0	Command was expanded to include the **ethernet y1731 meg**, **downspeed**, and **upspeed** parameters, as well as the Ethernet in the first mile (EFM) group interface.
Release R11.2.0	Command was expanded to include the High-level Data Link Control (HDLC) interface.
Release R11.5.0	Command was expanded to include the switchport interface, Gigabit Ethernet switchport interface, and 10-Gigabit Ethernet switchport interface.
Release R11.10.0	Command was expanded to include the **ip ffe entries less-than**, **ipv6 ffe entries less-than** and **voice user** <*extension*> **registered** parameters.

Functional Notes

There is no limit to how many probes, schedules, or interfaces can be tested within a single test list. However, only one type (AND, OR, or weighted) of test list can exist on a track at any given time.

An interface is IPv4 routing if its line-protocol state is up and if it has a valid, nonzero IPv4 address. This means that interfaces using Dynamic Host Configuration Protocol (DHCP) or negotiated Point-to-Point Protocol (PPP) will not pass until their primary IPv4 address is dynamically configured.

Usage Examples

The following example demonstrates use of the **test list weighted** command. The list contains three probe tests and each test has been assigned a different weight value (10, 20, and 30). When a probe test passes, its weight is added to the sum of the weights from other successful tests contained within the Weighted Track Test List. The pass threshold in this example is set to 35. The sum of all the weights must meet or exceed the value of 35 before the Weighted Track Test List will transition to a PASS state. The fail threshold in this example is set to 25. Therefore, if the sum of all the weights falls below the value of 25, the Weighted Track Test List will transition to a FAIL state.

(config)**#track LB-test**
(config-track)**#test list weighted**
(config-track-test)**#if probe LB weight 10**
(config-track-test)**#if probe LB2 weight 20**
(config-track-test)**#if probe LB3 weight 30**
(config-track-test)**#threshold pass 35 fail 25**
(config-track-test)**#exit**
(config-track)**#no shutdown**

The **show track LB-test** command is executed to see whether track LB-test is in a PASS state:

#show track LB-test
Current State: PASS (Admin: UP)
Testing:
+10 if probe LB (PASS)
+20 if probe LB2 (PASS)
+30 if probe LB3 (PASS)
Total = 60 currently, < 25 changes state to FAIL
Dampening Interval: 1 seconds
Time in current state: 2 days, 5 hours, 21 minutes, 13 seconds
Track State Changes: 0
Tracking:

Currently, all probe test commands are in the PASS state. Therefore, the sum of the assigned weights equals 60. The value of 60 exceeds the specified pass threshold of 35. As a result, the current state of the track is PASS.

Probe LB and probe LB3 have been forced to fail for demonstration purposes in this example. Output from the **show track LB-test** command shows track LB-test to be in a FAIL state.

(config-loop 1)**#do show track LB-test**
Current State: FAIL (Admin: UP)
Testing:
+10 if probe LB (FAIL)
+20 if probe LB2 (PASS)
+30 if probe LB3 (FAIL)
Total = 20 currently, >= 35 changes state to PASS
Dampening Interval: 1 seconds
Time in current state: 0 days, 0 hours, 0 minutes, 33 seconds
Track State Changes: 1
Tracking:

Only probe LB2 is in the PASS state. Therefore, the sum of the assigned weights equals 20. The value of 20 falls below the FAIL threshold of 25. As a result, the current state of the track is now FAIL.

time-schedule <*name*>

Use the **time-schedule** command to specify the time period a track has an effect. While the specified schedule is active, the track follows the state of its associated probe. Use the no form of this command to remove the time schedule from this track. Refer to the command *schedule <name> on page 1695* for more information on creating and modifying a schedule. Variations of this command include:

time-schedule <*name*> **pass**
time-schedule <*name*> **fail**

Syntax Description

<*name*>	Specifies the name of the time schedule to apply.
pass	Specifies that the track status is PASS when the schedule is inactive.
fail	Specifies that the track status is FAIL when the schedule is inactive.

Default Values

By default, no time schedule is assigned to the track. Therefore, the track always follows the state of its associated probe.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was expanded to allow specification of the track state when the schedule is inactive.

Usage Examples

The following example specifies that **schedule1** will be used to determine when **track1** follows the state of its probe:

(config)**#track track1**
(config-track)**#time-schedule schedule1 pass**

OSPFv2 and OSPFv3 Command Sets

This section includes the following command sets:

ROUTER OSPFV2 COMMAND SET

Open Shortest Path First version 2 (OSPFv2) is an Internet Protocol version 4 (IPv4) routing protocol defined in RFC 2328. The purpose of this protocol is to share the paths to destination networks among peer gateways or routers. The scope of operation for OSPF is designed to be within one autonomous system (AS). A single AS includes all routers normally under a single administrative control, rather than under the control of many autonomous systems, as with the Internet. OSPF is a hierarchical routing protocol, meaning it was developed to enable preplanning for large networks in a top-down fashion. This hierarchical structure allows a large network to be subdivided into smaller areas, which creates the ability to represent an entire area with a single network address, provides granular control over sensitive areas, creates smaller routing tables, reduces link-state exchanges, creates fewer shortest path first (SPF) calculations, and allows for larger internetworks. For more information about OSPF, refer to the technical note *Understanding OSPF*, available online at https://supportcommunity.adtran.com.

To activate the OSPF Configuration mode, enter the **router ospf** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router ospf
(config-ospf)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

area <area id> default-cost <value> on page 4122
area <area id> range <ipv4 address> <subnet mask> on page 4123
area <area id> stub on page 4124
auto-cost reference-bandwidth <value> on page 4125
default-information originate on page 4126
default-metric <value> on page 4127
distance <number> on page 4128
distribute-list <ipv4 acl name> out on page 4130
distribute-list route-map <name> in on page 4131
maximum-paths <value> on page 4132
network <ipv4 address> <wildcard mask> area <area id> on page 4133

area <*area id*> default-cost <*value*>

Use the **area default-cost** command to assign a cost of the default summary route sent into a stub area or not-so-stubby-area (NSSA). Use the **no** form of this command to delete the assigned cost.

Syntax Description

<*area id*>	Specifies an identifier for this area either as an integer (range is **0** to **4294967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*value*>	Specifies the default summary route cost. Range is **0** to **166777214**.

Default Values

By default, the summary route cost is set to **0**. There is no default for the area ID.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example defines a default cost of **85** to a specific area:

(config)**#router ospf**
(config-ospf)**#area 192.22.72.0 default-cost 85**

area *<area id>* **range** *<ipv4 address> <subnet mask>*

Use the **area range** command to configure area route summarizations and to determine whether an Internet Protocol version 4 (IPv4) address range is advertised to the networks. Use the **no** form of this command to disable this feature. Variations of this command include:

area *<area id>* **range** *<ipv4 address>* *<subnet mask>* **advertise**
area *<area id>* **range** *<ipv4 address>* *<subnet mask>* **not-advertise**

Syntax Description

<area id>	Specifies the identifier for this area. Specifies as an integer (range is **0** to **4294967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv4 address>	Specifies the IPv4 address of the advertised summary route. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
advertise	Specifies that the address range will be advertised to other networks.
not-advertise	Specifies that the address range will not be advertised to other networks.

Default Values

By default, open shortest path first (OSPF) is not enabled.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example defines an address range for a specific area that allows the unit to advertise this range to other networks:

(config)**#router ospf**
(config-ospf)**#area 11.0.0.0 range 11.0.0.0 255.0.0.0 advertise**

area <*area id*> stub

Use the **area stub** command to configure an area as a stub area. Use the **no** form of this command to disable stub-designation for areas defined as stubs using this command. Variations of this command include:

area <*area id*> **stub**
area <*area id*> **stub no-summary**

Syntax Description

<*area id*>	Specifies the identifier for this area. Specifies as an integer (range is **0** to **4294967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
no-summary	Optional. Designates the area as a total stub area. No summary link advertisements will be sent by the area border router (ABR) into the stub area.

Default Values

By default, open shortest path first (OSPF) is not enabled.

Command History

Release 3.1	Command was introduced.

Technology Review

It is important to coordinate configuration of all routers and access servers in the stub area. The **area stub** command must be configured for each of those pieces of equipment. Use the **area router configuration** command with the **area default-cost** command to specify the cost of a default internal router sent into a stub area by an ABR. Refer to *area <area id> default-cost <value> on page 4122* for related information.

Usage Examples

The following example configures **area 2** as a stub area:

(config)**#router ospf**
(config-ospf)**#area 2 stub**

auto-cost reference-bandwidth <*value*>

Use the **auto-cost reference-bandwidth** command to assign a different interface cost to an interface. It may be necessary to assign a higher number to high-bandwidth links. This value is used in open shortest path first (OSPF) metric calculations. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Sets the default reference bandwidth rate in Mbps. Range is **1** to **4294967** Mbps.

Default Values

By default, the rate is set to **100**.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example sets the auto cost reference bandwidth to **1000** Mbps:

(config)**#router ospf**
(config-ospf)**#auto-cost reference-bandwidth 1000**

default-information originate

Use the **default-information originate** command to cause an autonomous system boundary router (ASBR) to generate a default route. It must have its own default route before it generates one unless the **always** keyword is used. Use the **no** form of this command to return to the default setting. Variations of this command include:

default-information originate
default-information originate always
default-information originate always metric <*value*>
default-information originate always metric <*value*> **metric-type** <*type*>
default-information originate always metric <*value*> **metric-type** <*type*> **tag** <*value*>

*The optional parameters can be entered in any order. Use the **?** after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

always	Optional. Specifies to always advertise default route.
metric <*value*>	Optional. Configures the metric value. Range is **0** to **16777214**.
metric-type <*type*>	Optional. Configures the metric type. Select from type **1** or **2**.
tag <*value*>	Optional. Specifies the route tag for the default external route being injected. Route tags can be used to implement routing policies using route maps. For example, they can be used to control route redistribution to prevent routing loops when configuring multipoint route redistribution (i.e., routes are redistributed from protocol A into protocol B, then back into protocol A). Route tags only apply to external (Type 5) LSAs. Range is **1** to **4294967295**.

Default Values

By default, the metric value is set to **10** and the metric type is set to **2**.

Command History

Release 3.1	Command was introduced.
Release R11.3.0	Command syntax changed from **default-information-originate** to **default-information originate**.
Release R11.4.0	Command was expanded to include the **tag** parameter.

Usage Examples

The following example configures a router to always advertise default routes and assigns the default router a metric value of **10000** and a metric type of **2**:

(config)**#router ospf**
(config-ospf)**#default-information originate always metric 10000 metric-type 2**

default-metric *<value>*

Use the **default-metric** command to set a metric value for redistributed routes. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Sets the default metric value. Range is **0** to **4294967295**.

Default Values

By default, **default-metric** value is set at **20**.

Command History

Release 3.1	Command was introduced.

Functional Notes

The metric value defined using the **redistribute** command overrides the **default-metric** command's metric setting. Refer to *redistribute ospf on page 4215* for related information.

Usage Examples

The following example shows a router using both Routing Information Protocol (RIP) and open shortest path first (OSPF) routing protocols. The example advertises RIP-derived routes using the OSPF protocol and assigns the RIP-derived routes an OSPF metric of **10**.

(config)**#router ospf**
(config-ospf)**#default-metric 10**
(config-ospf)**#redistribute rip**

distance <*number*>

Use the **distance** command to overwrite the open shortest path first (OSPF) route administrative distance. This can be the same for all OSPF routes or different based on the route type. Use the **no** form of this command to set the OSPF administrative distance to the default value. Variations of this command include:

distance <*number*>
distance ospf external <*number*>
distance ospf intra-area <*number*>
distance ospf inter-area <*number*>

Syntax Description

<*number*>	Specifies the administrative distance to use when adding OSPF routes into the route table. Range is **0** to **255**.
ospf external	Specifies using a unique administrative distance for route paths between different autonomous systems (ASs).
ospf intra-area	Specifies using a unique administrative distance for route paths between a source and destination in the same routing area.
ospf inter-area	Specifies using a unique administrative distance for route paths between a source and destination in different areas.

Default Values

By default, **110** is the administrative distance for OSPF routes.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example configures external OSPF routes to use an administrative distance of **20** while other OSPF routes continue to use the default value of **110**:

(config)**#router ospf**
(config-ospf)**#distance ospf external 20**

Technology Review

An AS is a set of routers under common administration control that usually use a common routing strategy. Each AS is composed of routing areas, which are groups of adjoining networks and attached hosts. Intra-area routing occurs when the source and destination hosts are in the same area; inter-area routing occurs when the source and destination hosts are in different areas; and external routing occurs when communication is between different ASs.

Administrative distance is a feature that routers employ in order to select the most reliable path when there are two or more routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol by assigning a value (the smaller the value, the more trustworthy the protocol) that is then used by the router to organize routing protocols according to reliability.

distribute-list <*ipv4 acl name*> out

Use the **distribute-list out** command to apply an Internet Protocol version 4 (IPv4) access control list (ACL) to routes that are redistributed into the OSPFv2 network. Use the **no** form of this command to disable filtering.

For a complete list of all standard IPv4 ACL configuration commands, refer to the *IPv4 Access Control List Command Set on page 4252*.

Syntax Description

<ipv4 acl name>	Specifies an IPv4 ACL name. This is a standard IPv4 ACL against which the redistributed routes are matched.

Default Values

By default, distribute-list filtering is disabled.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

The **distribute-list** *<ipv4 acl name>* **out** command allows you to filter what traffic gets redistributed into the OSPFv2 network. For example, if the OSPFv2 process is configured to redistribute Routing Information Protocol (RIP) routes (using the command *redistribute on page 4134*), and RIP has a route to 10.22.8.0 /24, OSPFv2 would normally generate a Type 5 external LSA to distribute the route through the autonomous system (AS). However, if an ACL is applied that blocks the 10.22.8.0 /24 prefix, the external LSA will not be generated, and the route will not be distributed through the AS.

Usage Examples

The following example filters routes redistributed into the OSPFv2 process based on the ACL **RIP**:

(config)**#router ospf**
(config-ospf)**#distribute-list RIP out**

distribute-list route-map <*name*> in

Use the **distribute-list route-map in** command to apply a route map to filter the routes added by OSPFv2 to the route table. Use the **no** form of this command to disable filtering.

Syntax Description

<*name*>	Specifies a route map name.

Default Values

By default, distribute-list filtering is disabled.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

The **distribute-list route-map** <*name*> **in** command allows you to filter what OSPFv2 is allowed to add to the route table. For example, if OSPF calculations determine that a route to 10.22.8.0 /24 should be added to the route table, the route map matching rules are applied to the prefix to determine whether the route should be added to the route table. This command does not affect the distribution of link-state advertisements (LSAs) or the link-state (LS) database (every router in the same area should still have the same database for that area).

Usage Examples

The following example filters routes added to the OSPFv2 route table based on the route map **OSPFMAP**:

(config)**#router ospf**
(config-ospf)**#distribute-list route-map OSPFMAP in**

maximum-paths *<value>*

Use the **maximum-paths** command to specify the number of parallel routes (shared paths) open shortest path first (OSPF) can inject into the route table. When IP load sharing is enabled, traffic is balanced to a specific destination across up to six equal paths. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the number of routes OSPF can insert into the route table. Valid range is **1** to **6**.

Default Values

By default, the **maximum-paths** value is **4**.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the maximum number of multipath routes OSPF can insert in the route table to **5**.

(config)**#router ospf**
(config-ospf)**#maximum-paths 5**

network *<ipv4 address> <wildcard mask>* **area** *<area id>*

Use the **network area** command to enable routing on an IP stack and to define area IDs for the interfaces on which open shortest path first (OSPF) will run. Use the **no** form of this command to disable OSPF routing for interfaces defined using this command.

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<wildcard mask>	Specifies the wildcard mask that corresponds to a range of IPv4 addresses (network). Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
<area id>	Specifies the identifier for this area. Specifies as an integer (range is **0** to **4294967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

No default values are necessary for this command.

Command History

Release 3.1	Command was introduced.

Functional Notes

In order for OSPF to operate on an interface, the *primary* address for the interface must be included in the **network area** command. Assigning an interface to an OSPF area is done using the **network area** command. There is no limit to the number of **network area** commands used on a router. If the address ranges defined for different areas overlap, the first area in the **network area** command list is used and all other overlapping portions are disregarded. Try to avoid overlapping to avoid complications.

Usage Examples

In the following example, the OSPF routing process is enabled and two OSPF areas are defined:

(config)**#router ospf**
(config-ospf)**#network 192.22.72.101 0.0.0.255 area 0**
(config-ospf)**#network 10.0.0.0 0.255.255.255 area 10.0.0.0**

redistribute

Use the **redistribute** command to redistribute routes from a specified source into the Open Shortest Path First version 2 (OSPFv2) process. A router that performs redistribution becomes an OSPFv2 autonomous system boundary router (ASBR), because it is sourcing routes from outside the OSPFv2 autonomous system (AS). The specified source from which routes are redistributed must be in the same virtual routing and forwarding (VRF) as the OSPFv2 instance being configured. This command can be entered multiple times (at most, once for each source). Reentering the command with the same source replaces any existing command with that source. Use the **no** form of this command to remove the redistribution from the specified source. Variations of this command include:

redistribute bgp
redistribute bgp metric <*value*>
redistribute bgp metric-type <*type*>
redistribute bgp route-map <*name*>
redistribute bgp subnets
redistribute bgp tag <*value*>
redistribute connected
redistribute connected metric <*value*>
redistribute connected metric-type <*type*>
redistribute connected route-map <*name*>
redistribute connected subnets
redistribute connected tag <*value*>
redistribute ospf <*process id*>
redistribute ospf <*process id*> **metric** <*value*>
redistribute ospf <*process id*> **metric-type** <*type*>
redistribute ospf <*process id*> **no-include-connected**
redistribute ospf <*process id*> **route-map** <*name*>
redistribute ospf <*process id*> **tag** <*value*>
redistribute rip
redistribute rip metric <*value*>
redistribute rip metric-type <*type*>
redistribute rip route-map <*name*>
redistribute rip subnets
redistribute rip tag <*value*>
redistribute static
redistribute static metric <*value*>
redistribute static metric-type <*type*>
redistribute static route-map <*name*>
redistribute static subnets
redistribute static tag <*value*>

*The optional parameters can be entered in any order. Use the **?** after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

bgp	Specifies that Border Gateway Protocol (BGP) routes are being redistributed.
connected	Specifies that connected routes are being redistributed.
metric <*value*>	Optional. Specifies an OSPF metric value to be assigned to routes learned via BGP.
metric-type <*type*>	Optional. Specifies a type **1** or type **2** external route as the external link type. If not specified, the default is **2**.
ospf <*process id*>	Specifies the OSPF process from which to redistribute routes. Valid process ID range is **1** to **65535**.
no-include-connected	Optional. Specifies that prefixes of the interface running this source protocol are not automatically included in the route redistribution.
rip	Specifies that Routing Information Protocol (RIP) routes are being redistributed.
route-map <*name*>	Optional. Specifies a route map that is applied to routes being redistributed by this command. A route map can impose granular control on routes being redistributed.
static	Specifies that static routes are being redistributed.
subnets	Optional. Specifies subnet redistribution when redistributing routes into OSPF.
tag <*value*>	Optional. Specifies the route tag for the redistributed routes. Route tags can be used to implement routing policies using route maps. For example, they can be used to control route redistribution to prevent routing loops when configuring multipoint route redistribution (i.e., routes are redistributed from protocol A into protocol B, then back into protocol A). Route tags only apply to external (Type 5) LSAs. Range is **1** to **4294967295**.

Default Values

By default, this command is disabled.

Command History

Release 3.1	Command was introduced.
Release 10.1	Subcommands were added.
Release 14.1	Command was expanded to include the route map filtering.
Release R11.3.0	Command was expanded to include the **ospf** and **no-include-connected** parameters.
Release R11.4.0	Command was expanded to include the **tag** parameter.

Functional Notes

Redistributing routes imports those routes into OSPF without the interfaces in question actually participating in OSPF. The routes imported this way are not covered by a network command and do not send/receive OSPF traffic. This allows OSPF to learn and distribute routes to networks that do not participate in OSPF.

Usage Examples

The following example imports BGP routes into OSPF:

(config)**#router ospf**
(config-ospf)**#redistribute bgp**

rfc1583compatibility

Use the **rfc1583compatability** command to specify that the algorithm defined in RFC 1583 is used to determine autonomous system (AS) external routes. Use the **no** form of this command to specify that the algorithm defined in RFC 2328 is used to determine AS external routes.

Syntax Description

No subcommands.

Default Values

By default, RFC 1583 compatibility is enabled.

Command History

Release R11.4.0	Command was introduced.

Functional Notes

With the introduction of RFC 2328, the algorithm used to determine the cost of AS external routes was changed to help minimize the occurrence of routing loops.

This command should be set identically on all routers in the OSPFv2 network. Otherwise, the summary route from area boundary routers (ABRs) using RFC 1583 will be preferentially chosen because the summary routes they advertise will have a lower cost.

Usage Examples

The following example specifies that the algorithm defined in RFC 2328 is used to determine AS external routes:

(config)**#router ospf 5**
(config-ospf)**#no rfc1583compatibility**

router-id *<ipv4 address>*

Use the **router-id** command to specify the value to be used by the Open Shortest Path First version 2 (OSPFv2) process as the router ID. Use the **no** form of this command to return the router ID for this OSPFv2 process to the default value.

Syntax Description

<ipv4 address>	Specifies a 32-bit value, represented in IPv4 address format, that is used by this specific OSPFv2 instance as the router ID. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Valid IPv4 address range is **0.0.0.1** to **255.255.255.255**.

Default Values

The default router ID value is determined by algorithm (refer to *Functional Notes* below).

Command History

Release R11.3.0	Command was introduced.

Functional Notes

An OSPFv2 router ID is selected using a well-defined algorithm that is also used for Border Gateway Protocol (BGP) router IDs. The default router ID value is chosen by first looking at the configured router ID (if there is one), then the highest value IPv4 address assigned to a loopback interface in the same virtual routing and forwarding (VRF) instance that is not already in use as an OSPFv2 router ID (if there is one). Then, the highest value IPv4 address assigned to a non-loopback interface that is not already in use as an OSPFv2 router ID interface in the same VRF instance.

When defining an IPv4 address for the router ID, keep in mind that the value must be unique among router IDs in use by other OSPFv2 processes on the local system. If a value is specified that is already in use, an error message is displayed, and the command is rejected. Though the value uses an IPv4 address in general format, it does not actually use the IPv4 address.

Usage Examples

The following example specifies a router ID for the OSPFv2 process **5**:

(config)**#router ospf 5**
(config-ospf)**#router-id 10.10.10.2**

summary-address *<ipv4 address> <subnet mask>*

Use the **summary-address** command to control address summarization of routes that are redistributed into open shortest path first (OSPF) from other sources (for example, Routing Information Protocol (RIP)-to-OSPF, static-to-OSPF, etc.). Variations of this command include:

summary-address *<ipv4 address> <subnet mask>*
summary-address *<ipv4 address> <subnet mask>* **not-advertise**
summary-address *<ipv4 address> <subnet mask>* **tag**

*The optional parameters can be entered in any order. Use the **?** after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).
not-advertise	Optional. Causes suppression of routes that match the specified IPv4 address and subnet mask.
tag *<value>*	Optional. Specifies the route tag for the summarized route. Route tags can be used to implement routing policies using route maps. For example, they can be used to control route redistribution to prevent routing loops when configuring multipoint route redistribution (i.e., routes are redistributed from protocol A into protocol B, then back into protocol A). Route tags only apply to external (Type 5) LSAs. Range is **1** to **4294967295**.

Default Values

By default, this command is disabled.

Command History

Release 3.1	Command was introduced.
Release R11.4.0	Command was expanded to include the **tag** parameter.

Usage Examples

The following example suppresses advertisement of the routes that match the specified IPv4 address and subnet mask:

(config)**#router ospf**
(config-ospf)**#summary-address 11.0.0.0 255.0.0.0 not-advertise**

timers spf <*delay*> <*hold*>

Use the **timers spf** command to configure the shortest path first (SPF) calculation and hold intervals. Use the **no** form of this command to return to the default setting. Variations of this command include:

timers spf <*delay*>
timers spf <*delay*> <*hold*>

Syntax Description

<*delay*>	Specifies the time in seconds between open shortest path first's (OSPF's) receipt of topology changes and the beginning of SPF calculations.
<*hold*>	Specifies the time in seconds between consecutive SPF calculations. Range is **10** to **1800** seconds.

Default Values

By default, the SPF delay is **5** seconds and the hold interval is set to **10** seconds.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example defines a delay of **10** seconds and a hold time of **30** seconds:

(config)**#router ospf**
(config-ospf)**#timers spf 10 30**

ROUTER OSPFV3 COMMAND SET

Open Shortest Path First version 3 (OSPFv3) is the newest version of OSPF and includes Internet Protocol version 6 (IPv6) support by using IPv6 messages to calculate IPv6 routes. Dual stack networks can use an OSPFv2 instance to support IPv4 connectivity and an OSPFv3 instance to support IPv6 connectivity. OSPFv3 functions by allowing routers to resolve paths through the network using OSPFv3 messages sent over IPv6 packets. OSPFv3 functions in a similar manner to OSPFv2, with a few crucial exceptions. In OSPFv3 for IPv6, authentication has been removed from the OSPF protocol. When running over IPv6, OSPF relies on the IP Encapsulating Security Payload (ESP) and IP Authentication Header (AH) protocols to ensure integrity and authentication or confidentiality of routing exchanges (refer to RFC 4552). In addition, all addressing semantics have been removed from OSPF packet headers in OSPFv3. All addressing information is contained in the various link state advertisements (LSA) types only. In OSPFv3, neighboring routers are always identified by router ID, rather than by an IPv4 address as with OSPFv2. In OSPFv2, unknown LSAs were discarded. In OSPFv3, however, the protocol allows a mixture of router capabilities on a single link, so these LSAs are not discarded but rather can be handled more flexibly.

Another major difference between OSPFv2 and OSPFv3 is that in OSPFv3, the concept of address families is introduced. Address families use entirely separate OSPF processes for each family. Each process maps its messages to or from the wire using a different instance ID. OSPFv3 address families are configured once routing for the address family is enabled at the global level. Configuration commands for OSPFv3 address families are discussed in *Router OSPFv3 IPv6 Address Family on page 4153*.

There are many additional differences between OSPFv2 and OSPFv3 operation and configuration. For more information about OSPFv3 configuration, refer to the configuration guide *Configuring IPv6 in AOS*, available online at http://supportforums.adtran.com.

To activate the OSPF Configuration mode, enter the **router ospfv3** <*process id*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router ospfv3 5
(config-ospfv3)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

address-family ipv6 unicast on page 4143
area <area id> authentication ipsec spi <spi> on page 4144
area <area id> default-cost <value> on page 4146
area <area id> encryption ipsec spi <spi> on page 4147
area <area id> stub on page 4149

address-family ipv6 unicast

Use the **address-family ipv6 unicast** command to specify an address family for the Open Shortest Path First version 3 (OSPFv3) process, and to enter the address family's configuration mode. Once an address family is created, it is permanently associated with the parent OSPFv3 process until the process itself is removed. Therefore, there is not a **no** version of this command.

Syntax Description

No subcommands.

Default Values

By default, no address family exists.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example creates an IPv6 address family for the OSPFv3 process **5**:

```
(config)#router ospfv3 5
(config-ospfv3)#address-family ipv6 unicast
```

area <*area id*> authentication ipsec spi <*spi*>

Use the **area authentication ipsec spi** command to enable authentication of all Open Shortest Path First version 3 (OSPFv3) messages that are sent or received on each interface in the specified area and to specify the authentication type. This command allows you to specify OSPFv3 authentication at the area level, which eases configuration and management when the same security settings are desired at multiple interfaces. It also allows the same security parameter index (SPI) to be used at multiple interfaces, which is not possible when specifying OSPFv3 authentication at the interface level. Use the **no** form of this command to remove IP security (IPsec) authentication of OSPFv3 messages in the area. Variations of this command include:

area <*area id*> **authentication ipsec spi** <*spi*> **md5** <*key*>
area <*area id*> **authentication ipsec spi** <*spi*> **sha1** <*key*>

Syntax Description

area <*area id*>	Specifies the ID of the area on which authentication is used. The area is specified as an integer (range is **1** to **967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
ipsec	Specifies that IPsec authentication is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by another IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
md5 <*key*>	Specifies that Message-Digest 5 (**md5**) is used for authentication. Keys are specified as 32 hexadecimal characters.
sha1 <*key*>	Specifies that secure-Hash 1 (**sha1**) is used for authentication. Keys are specified as 40 hexadecimal characters.

Default Values

By default, there is no authentication for OSPFv3 messages in an area.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages in area **10** with an SPI of **100** and **md5** as the authentication method:

(config)**#router ospfv3 5**
(config-ospfv3)**#area 10 authentication ipsec spi 100 md5 NeWtStpsswdKEY**

area <*area id*> default-cost <*value*>

Use the **area default-cost** command to assign a cost of the default summary route sent into a stub area or not-so-stubby-area (NSSA). Use the **no** form of this command to delete the assigned cost.

Syntax Description

<*area id*>	Specifies an identifier for this area either as an integer (range is **1** to **967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*value*>	Specifies the default summary route cost. Range is **0** to **166777214**.

Default Values

By default, the summary route cost is set to **0**. There is no default for the area ID.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example defines a default cost of **85** to a specific area:

(config)**#router ospfv3 5**
(config-ospfv3)**#area 192.22.72.0 default-cost 85**

area <*area id*> encryption ipsec spi <*spi*>

Use the **area encryption ipsec spi** command to specify a symmetrical, bidirectional Open Shortest Path First version 3 (OSPFv3) security association (SA) that uses encapsulating security payload (ESP) for encryption and authentication of all OSPFv3 messages that are sent or received on each interface in the specified area. This command allows you to specify OSPFv3 security at the area level, which eases configuration and management when the same security settings are desired at multiple interfaces. It also allows the same security parameter index (SPI) to be used at multiple interfaces, which is not possible when specifying OSPFv3 protection at the interface level. Use the **no** form of this command to remove IP security (IPsec) protection of OSPFv3 messages in the area. Variations of this command include:

area <*area id*> **encryption ipsec spi** <*spi*> **esp** <*encryption type*> <*encryption key*> <*authentication type*> <*authentication key*>

area <*area id*> **encryption ipsec spi** <*spi*> **esp null** <*authentication type*> <*authentication key*>

Syntax Description

area <*area id*>	Specifies the ID of the area on which encryption and authentication is used. The area is specified as an integer (range is **1** to **967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
ipsec	Specifies that IPsec encryption is used on the interface for OSPFv3 SAs.
spi <*spi*>	Specifies the security parameter index (SPI) for the SA. The value specified must not be in used by another IPsec function on the system, or an error message is generated. If the same SPI is already in use in the same OSPFv3 area, entering this command with the same value will overwrite the current configuration. Valid SPI range is **256** to **4294967295**.
esp	Specifies that ESP is used.
null	Specifies that OSPFv3 messages on this interface are not encrypted when used in the **ospfv3 encryption null** format (even when encryption is specified by the OSPFv3 area configuration). When used in the **ospfv3 encryption ipsec spi** <*spi*> **esp null** format, **null** indicates that messages on the interface will not be encrypted, but will be authenticated.
<*encryption type*>	Specifies the type of algorithm used to encrypt OSPFv3 messages. Valid values for encryption are: **3des** uses triple data encryption standard (DES). **aes-cbc** uses advanced encryption standard (AES) with cipher block chaining (CBC). Select from **aes-cbc 128**, **aes-cbc 192**, or **aes-cbc 256**. **des** uses DES.
<*encryption key*>	Specifies the hexadecimal encryption key. The size of the encryption key is determined by the respective encryption algorithm, as follows: **3des** uses a **48** character key size. **aes-cbc 128** uses a **32** character key size. **aes-cbc 192** uses a **48** character key size.

aes-cbc 256 uses a **64** character key size.

des uses a **16** character key size.

<authentication type> Specifies the algorithm used for authenticating OSPFv3 messages. Valid values for authentication are Message-Digest 5 (**md5**) and Secure-Hash 1 (**sha1**) algorithms.

<authentication key> Specifies the hexadecimal authentication key. The size of the authentication key is determined by the respective authentication algorithm, as follows:

md5 uses a **32** character key size.

sha1 uses a **40** character key size.

Default Values

By default, there is no security for OSPFv3 messages in an area.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

This commands specifies OSPFv3 security at the area level. After this command has been entered, and the security associations (SAs) are in place, if the command is reentered with different settings, an attempt is made to create the new SA. If SA creation fails, an error message is displayed, the command is not accepted into the running configuration on the device, and the original command and SAs remain in place. When OSPFv3 protection is specified at multiple locations that affect the same interface, one protection set is selected to protect all OSPFv3 instances on that interface. The set is chosen using the following rules processed in this order:

1. The protection configured at the interface level (including null), then everything else
2. The protection configured at the IPv6 address family instance, then everything else
3. The protection configured at the IPv4 address family instance, then everything else (IPv4 address family is not supported as of AOS firmware release R10.5.0).
4. No protection.

For more information about configuring OSPFv3, refer to the configuration guide *Configuring IPv6 in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures OSPFv3 messages in area **10** with an SPI of **100**, no encryption, and **md5** as the authentication method:

```
(config)#router ospfv3 5
(config-ospfv3)#area 10 encryption ipsec spi 100 esp null md5 NeWtStpsswdKEY
```


area <*area id*> stub

Use the **area stub** command to configure an area as a stub or total stub area. When an area is specified as a stub, the area border router withholds inter-area-router link state advertisements (LSAs) and autonomous system (AS)-external LSAs, and instead injects a default summary route. When an area is a total stub, the area border router also withholds inter-area-prefix LSAs. The cost for the injected route is defined by the command *area <area id> default-cost <value> on page 4146*. Use the **no** form of this command to return the area to the default area type. Variations of this command include:

area <*area id*> **stub**
area <*area id*> **stub no-summary**

Syntax Description

<area id>	Specifies the identifier for this area. Area IDs are specified as an integer (range is **1** to **967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
no-summary	Optional. Designates the area as a total stub area.

Default Values

By default, the area type is normal, and is not specified as a stub.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example configures area **10** as a total stub area:

(config)**#router ospfv3 5**
(config-ospfv3)**#area 10 stub no-summary**

auto-cost reference-bandwidth <*value*>

Use the **auto-cost reference-bandwidth** command to specify the reference value used to calculate the Open Shortest Path First version 3 (OSPFv3) cost of an interface. In OSPFv3, the cost of an interface is the reference value divided by the interface's bandwidth. Certain conditions require a change to the system's reference value, such as an increase in interface speeds. This command allows the reference value to be customized for specific network requirements. All OSPFv3 participants in the network should use the same reference value. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Sets the default reference bandwidth rate in Mbps. This rate is used to calculate the OSPFv3 cost on the AOS device's OSPFv3 interfaces. Range is **1** to **4294967** Mbps.

Default Values

By default, the rate is set to **100** Mbps.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example sets the auto cost reference bandwidth to **1000** Mbps:

(config)**#router ospfv3 5**
(config-ospfv3)**#auto-cost reference-bandwidth 1000**

router-id *<ipv4 address>*

Use the **router-id** command to specify the value to be used by the Open Shortest Path First version 3 (OSPFv3) process as the router ID. Use the **no** form of this command to return the router ID for this OSPFv3 process to the default value.

Syntax Description

<ipv4 address>	Specifies a 32-bit value, represented in IPv4 address format, that is used by this specific OSPFv3 instance as the router ID. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). Valid IPv4 address range is **0.0.0.1** to **255.255.255.255**.

Default Values

The default router ID value is determined by algorithm (refer to *Functional Notes* below).

Command History

Release R10.5.0	Command was introduced.

Functional Notes

An OSPFv3 router ID is selected using a well-defined algorithm that is also used for Border Gateway Protocol (BGP) router IDs. The default router ID value is chosen by first looking at the configured router ID (if there is one), then the highest value IPv4 address assigned to a loopback interface in the same virtual routing and forwarding (VRF) instance that is not already in use as an OSPFv3 router ID (if there is one). Then, the highest value IPv4 address assigned to a non-loopback interface that is not already in use as an OSPFv3 router ID interface in the same VRF instance.

When defining an IPv4 address for the router ID, keep in mind that the value must be unique among router IDs in use by other OSPFv3 processes on the local system. If a value is specified that is already in use, an error message is displayed, and the command is rejected. Though the value uses an IPv4 address in general format, it does not actually use the IPv4 address.

Usage Examples

The following example specifies a router ID for the OSPFv3 process **5**:

(config)**#router ospfv3 5**
(config-ospfv3)**#router-id 10.10.10.2**

timers spf <*delay*>

Use the **timers spf** command to configure the Open Shortest Path First version 3 (OSPFv3) shortest path first (SPF) calculation and hold interval timers. Use the **no** form of this command to return the timers to the default settings. Variations of this command include:

timers spf <*delay*>
timers spf <*delay*> <*hold*>

Syntax Description

<*delay*>	Specifies the time in seconds between receipt of OSPFv3 topology changes and the beginning of SPF calculations. Valid range is **0** to **65535** seconds.
<*hold*>	Optional. Specifies the time in seconds between consecutive SPF calculations. Range is **0** to **65535** seconds.

Default Values

By default, the SPF delay is **5** seconds and the hold interval is **10** seconds.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example defines an SPF delay timer of **10** seconds:

(config)**#router ospfv3 5**
(config-ospfv3)**#timers spf 10**

ROUTER OSPFV3 IPV6 ADDRESS FAMILY

In Open Shortest Path First version 3 (OSPFv3), the concept of address families is introduced. Address families use entirely separate OSPFv3 processes for each family. Each OSPFv3 process maps its messages to or from the wire using a different instance ID. The instance ID is a field in the OSPF header with a value from **0** to **255**. The value itself conveys no information, other than the instance number; however, the instance ID adheres to a range of values that convey address family information (refer to RFC 5838). The table below outlines the address family information associated with each instance ID value.

Instance ID Range	Address Family	Default Value
0 to 31	IPv6 Unicast	0
32 to 63	IPv6 Multicast	32
64 to 95	IPv4 Unicast	64
96 to 127	IPv4 Multicast	96
128 to 255	Unassigned	

*As of AOS firmware release R10.5.0, only IPv6 unicast address families are supported for OSPFv3. This configuration is backward compatible with non-address family capable OSPFv3 devices that support only IPv6, as long as those devices use the instance ID for the **Base IPv6 Unicast AF** (value of **0**). The AOS unit only accepts OSPF messages that do not set the address family bit when the instance ID is 0.*

Before an OSPFv3 process address family can be created, routing for the address family must be enabled at the global level (using the command *ipv6 unicast-routing on page 1564*). Before an OSPFv3 process can be enabled at an interface, routing for the address family must be enabled at that interface (using the command **ipv6** or a variation of the **ipv6 address** command). Globally disabling routing for an address family does not remove existing OSPFv3 commands associated with that address family. Disabling an address family at an interface removes OSPFv3 commands associated with that address family at the interface.

Because an OSPFv3 process supports one address family, and only one instance of an address family is allowed at an interface, all **ospfv3** <*process id*> commands entered at a given interface must have the same value for the process ID. In addition, OSPFv3 for a given process ID must be globally enabled before **ospfv3** <*process id*> commands can be entered at the interface.

For more information about OSPFv3 configuration, refer to the configuration guide *Configuring IPv6 in AOS*, available online at http://supportforums.adtran.com

To create an OSPFv3 address family, and enter the address family configuration mode, enter the **address-family ipv6 unicast** command from the OSPFv3 Configuration mode as follows:

```
(config)#router ospfv3 5
(config-ospfv3)#address-family ipv6 unicast
(config-ospfv3-ipv6)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

area <area id> range <ipv6 address/prefix-length> on page 4155
default-information originate on page 4156
default-metric <value> on page 4158
distance <number> on page 4159
duplicate-routerid-detection on page 4161
maximum-paths <value> on page 4162
redistribute on page 4163
summary-prefix <ipv6 address/prefix-length> on page 4166

area *<area id>* **range** *<ipv6 address/prefix-length>*

Use the **area range** command to control the route summarization between Open Shortest Path First version 3 (OSPFv3) areas (inter-area prefixes of type 3 link-state advertisements (LSAs)). Use the **no** form of this command to remove the specified summarization, and return to advertisement of individual summary prefixes between areas. Variations of this command include:

area *<area id>* **range** *<ipv6 address/prefix-length>*
area *<area id>* **range** *<ipv6 address/prefix-length>* **advertise**
area *<area id>* **range** *<ipv6 address/prefix-length>* **not-advertise**

Syntax Description

<area id>	Specifies the identifier of the area of which the router is a member, and which contains the prefixes being summarized. Specify area IDs as an integer (range is **1** to **967295**) or an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address/prefix-length>	Specifies the IPv6 prefix and length to be advertised. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
advertise	Optional. Specifies that the summary will be advertised to other OSPFv3 areas.
not-advertise	Optional. Specifies that the summary will not be advertised to other OSPFv3 areas.

Default Values

By default, route summarization is disabled. When enabled, OSPFv3 route summaries are advertised by default.

Command History

Release 3.1	Command was introduced.
Release R10.5.0	Command was expanded to include OSPFv3 functionality and the OSPFv3 IPv6 address family.

Functional Notes

Operation of this command is the same as the existing OSPFv2 command (*area <area id> range <ipv4 address> <subnet mask> on page 4123*), with the exception that the range is specified as an Internet Protocol version 6 (IPv6) prefix and length, rather than an IPv4 address with subnet and mask.

Usage Examples

The following example configures route summarization between OSPFv3 areas:

(config-ospfv3)**#address-family ipv6 unicast**
(config-ospfv3-ipv6)**#area 10 range 2001:DB8::1/64 not-advertise**

default-information originate

Use the **default-information originate** command to specify that a default external route is injected into the Open Shortest Path First version 3 (OSPFv3) process. A router that injects an external default route becomes an OSPFv3 autonomous system border router (ASBR) because it sources routes from outside the OSPFv3 autonomous system (AS). Use the **no** form of this command to remove the external default route. Variations of this command include:

default-information originate
default-information originate always
default-information originate metric <*value*>
default-information originate metric-type 1
default-information originate metric-type 2

Syntax Description

always	Optional. Specifies that the injected default route is always advertised.
metric <*value*>	Optional. Assigns an OSPFv3 metric value to the route being injected into OSPFv3. Valid metric range is **0** to **16777214**.
metric-type 1	Optional. Specifies the external metric type for the route being injected into OSPFv3. Metric type **1** specifies that when external routes are assigned a metric they begin with the metric value specified by this command, and add the cost of the OSPF path as they are advertised throughout the AS.
metric-type 2	Optional. Specifies the external metric type for the route being injected into OSPFv3. Metric type **2** is not affected by the OSPF path cost, and retains the original metric values.

Default Values

By default, no external routes are injected into OSPFv3. When an external route is injected, by default it will use **metric-type 2**, and will have a metric value that is the same as the default metric set by the command *default-metric <value> on page 4158*. If the default metric command is not configured, the injected route will have a default metric of **10** (refer to *Functional Notes* below).

Command History

Release 3.1	Command was introduced.
Release R10.5.0	Command was expanded to include OSPFv3 functionality and the OSPFv3 IPv6 address family.

Functional Notes

If the metric is not specified, then the **default-metric** command is used for the default route metric (refer to *default-metric <value> on page 4158*). If the **default-metric** command is not configured, then a metric of **10** is used. If the metric is specified as **0** using the **default-information originate** command, it means that the metric is set to an unconfigured value, and the **default-metric** command setting is used.

Usage Examples

The following example specifies that an external route is injected into OSPFv3 using the default metric value of **10** and the default metric type of **2**:

(config-ospfv3)**#address-family ipv6 unicast**
(config-ospfv3-ipv6)**#default-information originate always**

default-metric *<value>*

Use the **default-metric** command to specify the metric value used for Open Shortest Path First version 3 (OSPFv3) redistributed routes when the value is not otherwise specified. The metric for redistributed routes can be specified using the command *redistribute on page 4163* or using a route map. When the value is not set in one of the locations, the default metric is used. This setting does not affect the metric of the default route injected using the command *default-information originate on page 4156*, although this value is used if the metric is not specified in the **default-information originate** command. Use the **no** form of this command to return the default metric to the default value.

Syntax Description

<value>	Specifies the OSPFv3 metric value assigned to the route being injected into OSPFv3. Valid range is **0** to **6777214**.

Default Values

By default, the default metric is set to **20**.

Command History

Release 3.1	Command was introduced.
Release R10.5.0	Command was expanded to include OSPFv3 functionality and the OSPFv3 IPv6 address family.

Usage Examples

The following example changes the default metric to **30**:

```
(config-ospfv3)#address-family ipv6 unicast
(config-ospfv3-ipv6)#default-metric 30
```


distance <*number*>

Use the **distance** command to specify the administrative distance for Open Shortest Path First version 3 (OSPFv3) routes. The distance can be set once for all OSPFv3 route types or individually for each route type. Use the **no** form of this command to return the administrative distance to the default value. Variations of this command include:

distance <*number*>
distance ospf external <*number*>
distance ospf inter-area <*number*>
distance ospf intra-area <*number*>

Syntax Description

<*number*>	Specifies the administrative distance to use when adding OSPFv3 routes into the route table. Range is **0** to **255**.
ospf intra-area	Optional. Specifies using a unique administrative distance for route paths between a source and destination in the same routing area.
ospf inter-area	Optional. Specifies using a unique administrative distance for route paths between a source and destination in different areas.
ospf external	Optional. Specifies using a unique administrative distance for route paths between different autonomous systems.

Default Values

By default, **110** is the administrative distance for OSPFv3 routes.

Command History

Release 15.1	Command was introduced.
Release R10.5.0	Command was expanded to include OSPFv3 functionality and the OSPFv3 address family.

Usage Examples

The following example changes the administrative distance of all OSPFv3 routes to **150**:

(config-ospfv3)**#address-family ipv6 unicast**
(config-ospfv3-ipv6)**#distance 150**

Technology Review

An autonomous system (AS) is a set of routers under common administration control that usually use a common routing strategy. Each AS is composed of routing areas, which are groups of adjoining networks and attached hosts. Intra-area routing occurs when the source and destination hosts are in the same area; inter-area routing occurs when the source and destination hosts are in different areas; and external routing occurs when communication is between different ASs.

Administrative distance is a feature that routers employ in order to select the most reliable path when there are two or more routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol by assigning a value (the smaller the value, the more trustworthy the protocol) that is then used by the router to organize routing protocols according to reliability.

duplicate-routerid-detection

Use the **duplicate-routerid-detection** command to enable the ability to detect when a duplicate router ID is found in the Open Shortest Path First version 3 (OSPFv3) link state database. When enabled, if a received link state advertisement (LSA) contains the router ID of the OSPFv3 process to which the LSA belongs, a warning event is displayed. Use the **no** form of this command to disable duplicate router ID detection.

Syntax Description

No subcommands.

Default Values

By default, duplicate router ID detection is disabled.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example enables duplicate router ID detection for the OSPFv3 address family:

```
(config-ospfv3)#address-family ipv6 unicast
(config-ospfv3-ipv6)#duplicate-routerid-detection
```

maximum-paths *<value>*

Use the **maximum-paths** command to specify the maximum number of equal cost routes to a given prefix that Open Shortest Path First version 3 (OSPFv3) can enter into the route table. Use the **no** form of this command to return the maximum paths value to the default setting.

Syntax Description

<value>	Specifies the maximum number of equal cost OSPFv3 routes allowed. Valid range is **1** to **6**.

Default Values

By default, the **maximum-paths** value is **4**.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was expanded to include OSPFv3 functionality and the OSPFv3 IPv6 address family.

Usage Examples

The following example sets the maximum number of equal cost routes to **5**:

(config-ospfv3)**#address-family ipv6 unicast**
(config-ospfv3-ipv6)**#maximum-paths 5**

redistribute

Use the **redistribute** command to redistribute routes from a specified source into the Open Shortest Path First version 3 (OSPFv3) process. A router that performs redistribution becomes an OSPFv3 ASBR, because it is sourcing routes from outside the OSPFv3 AS. The specified source from which routes are redistributed must be in the same virtual routing and forwarding (VRF) instance, and of the same address family as the OSPFv3 instance being configured. This command can be entered multiple times (at most, once for each source). Reentering the command with the same source replaces any existing command with that source. Use the **no** form of this command to remove the redistribution from the specified source. Variations of this command include:

redistribute bgp
redistribute bgp metric <*value*>
redistribute bgp metric-type 1
redistribute bgp metric-type 2
redistribute bgp route-map <*map*>
redistribute connected
redistribute connected metric <*value*>
redistribute connected metric-type 1
redistribute connected metric-type 2
redistribute connected route-map <*map*>
redistribute ospf <*process id*>
redistribute ospf <*process id*> **include-connected**
redistribute ospf <*process id*> **metric** <*value*>
redistribute ospf <*process id*> **metric-type 1**
redistribute ospf <*process id*> **metric-type 2**
redistribute ospf <*process id*> **route-map** <*map*>
redistribute static
redistribute static metric <*value*>
redistribute static metric-type 1
redistribute static metric-type 2
redistribute static route-map <*map*>

Syntax Description

bgp	Specifies that Border Gateway Protocol (BGP) routes are being redistributed.
connected	Specifies that connected routes are being redistributed.
ospf <*process id*>	Specifies the OSPF process from which to redistribute routes. Valid process ID range is **1** to **65535.**
include-connected	Optional. Specifies that all connected routes corresponding with the OSPF process are redistributed. In addition, routes on interfaces participating in the OSPF process are also redistributed.
static	Specifies that static routes are being redistributed.
metric <*value*>	Optional. Assigns an OSPFv3 metric value to the route being redistributed into OSPFv3. Valid metric range is **0** to **16777214**.

metric-type 1	Optional. Specifies the external metric type for the route being redistributed into OSPFv3. Metric type **1** specifies that when external routes are assigned a metric they begin with the metric value specified by this command, and add the cost of the OSPF path as they are advertised throughout the autonomous system.
metric-type 2	Optional. Specifies the external metric type for the route being redistributed into OSPFv3. Metric type **2** is not affected by the OSPF path cost, and retains the original metric values.
route-map *<map>*	Optional. Specifies a route map that is applied to routes being redistributed by this command. A route map can impose granular control on routes being redistributed.

Default Values

By default, no routes are redistributed into OSPFv3. When a route is redistributed, by default it will use **metric-type 2**, and will have a metric value that is the same as the default metric set by the command *default-metric <value> on page 4158*. If the default metric command is not configured, the injected route will have a default metric of **10** (refer to *Functional Notes* below).

Command History

Release 3.1	Command was introduced.
Release 14.1	Command was expanded to include the **bgp** keyword and route map filtering.
Release R10.5.0	Command was expanded to include the OSPFv3 functionality and the OSPFv3 IPv6 address family.
Release R10.8.0	Command was expanded to include the **ospf** and **include-connected** parameters.

Functional Notes

The optional parameters of this command can be entered in any order.

When using redistribution, keep in mind the following:

- OSPFv3 settings, such as metric and metric types, that are specified in a route map entry override those settings in the **redistribution** command for the routes that match the route map entry.
- When using the command *summary-prefix <ipv6 address/prefix-length> on page 4166*, individual routes that are summarized, as well as the resulting summary, bypass route maps in **redistribute** commands.
- By default, no route map is used.

If the metric is not specified, then the **default-metric** command is used for the default route metric (refer to *default-metric <value> on page 4158*). If the **default-metric** command is not configured, then a metric of **10** is used. If the metric is specified as **0** using the **default-information originate** command, it means that the metric is set to an unconfigured value, and the **default-metric** command setting is used.

Usage Examples

The following example redistributes all routes from BGP:

(config-ospfv3)#**address-family ipv6 unicast**
(config-ospfv3-ipv6)#**redistribute bgp**

summary-prefix *<ipv6 address/prefix-length>*

Use the **summary-prefix** command to control route summarization and route advertisement that is redistributed into this Open Shortest Path First version 3 (OSPFv3) process (external prefixes of type 5 link state advertisements (LSAs)). Use the **no** form of this command to remove the specified route summary, and return to advertising the individual prefixes that are being redistributed. Variations of this command include:

summary-prefix *<ipv6 address/prefix-length>*
summary-prefix *<ipv6 address/prefix-length>* **not-advertise**

Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 prefix and length to be advertised. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
not-advertise	Optional. Specifies that the summary is not advertised to other OSPFv3 areas.

Default Values

By default, the cost applied to the summary route is that of the lowest cost route in the set it summarizes.

Command History

Release R10.5.0	Command was introduced.

Functional Notes

The command can be entered multiple times to summarize different prefixes. Individual routes being summarized, as well as the resulting summary prefix, bypass route maps specified in the *redistribute on page 4163* commands. In addition, if multiple summaries exist where one summary subsumes another, the prefix with the shortest length is used.

Usage Examples

The following example creates a route summary:

(config-ospfv3)**#address-family ipv6 unicast**
(config-ospfv3-ipv6)**#summary-prefix 2001:DB8::1/64**

ROUTING COMMAND SETS

This section includes the following command sets:

ROUTE MAP COMMAND SET

The Route Map Command Set contains commands used to match attributes within a route for the purpose of filtering. This section also contains set commands that are optionally used to apply attributes to the routes that are being filtered.

To activate the Route Map Configuration mode, enter the **route-map** command at the Global Configuration mode prompt. Refer to the command *route-map on page 1687* for additional information.

For example:

```
>enable
#configure terminal
(config)#route-map MyMap permit 100
(config-route-map)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

match as-path <name> on page 4170
match community <name> on page 4171
match ip address <name> on page 4172
match ip address prefix-list <name> on page 4173
match ip dscp on page 4174
match ip precedence on page 4178
match ipv6 address <ipv6 acl name> on page 4180
match ipv6 address prefix-list <name> on page 4181
match length <minimum> <maximum> on page 4182
match metric <value> on page 4183
match tag <number> on page 4184
set as-path prepend on page 4185
set comm-list <name> delete on page 4186
set community on page 4187
set default interface on page 4189
set interface <interface> on page 4190

match as-path *<name>*

Use the **match as-path** command to configure the route map to route traffic based on the autonomous system (AS) path list name. Use the **no** form of this command to discontinue matching.

Syntax Description

<name>	Specifies the name of the AS path list you want to match.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match the AS path list named **TESTPATH**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match as-path TESTPATH**

match community <*name*>

Use the **match community** command to configure the route map to route traffic based on a specified community. Use the **no** form of this command to discontinue matching. Variations of this command include:

match community <*name*>
match community <*name*> **exact-match**

Syntax Description

<*name*>	Specifies the name of the community you want to match.
exact-match	Optional. Specifies that the route map must match the community name exactly.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match the community named **MYCOMMUNITY**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match community MYCOMMUNITY**

match ip address <*name*>

Use the **match ip address** command to configure the route map to route traffic based on the access control list (ACL) name defined with the **ip access-list** command. Refer to *ip access-list standard <ipv4 acl name> on page 1346* for more information. Use the **no** form of this command to discontinue matching.

Syntax Description

<name>	Specifies the name of the ACL to match.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match the IP address ACL named **MYLIST**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match ip address MYLIST**

match ip address prefix-list *<name>*

Use the **match ip address prefix-list** command to configure the route map to route traffic based on a prefix list route filter. The name of the prefix list is defined with the **ip prefix-list** command. Refer to *ip prefix-list <name> description "<text>" on page 1442* for more information. Use the **no** form of this command to discontinue matching.

Syntax Description

<name>	Specifies matching the IP address based on the prefix list name.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match the IP address prefix list named **MYLIST**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match ip address prefix-list MYLIST**

match ip dscp

Use the **match ip dscp** command to configure the route map to route traffic based on the differentiated services code point (DSCP) value in the IP header of the packet. Use the **no** form of this command to discontinue matching. Variations of this command include:

match ip dscp <*value*>
match ip dscp af*xx*
match ip dscp cs*x*
match ip dscp default
match ip dscp ef

Syntax Description

<*value*>	Specifies the DSCP numeric value. Valid range is **0** to **63**.
af*xx*	Specifies the assured forwarding (AF) class and subclass. Select from: 11 (001010), 12 (001100), 13 (001110), 21 (010010), 22 (010100), 23 (010110), 31 (011010), 32 (011100), 33 (011110), 41 (100010), 42 (100100), or 43 (100110).
cs*x*	Specifies the class selector (CS) value. Valid range is **1** to **7**.
default	Specifies the default IP DSCP value (000000).
ef	Specifies marking for expedited forwarding (EF).

Default Values

No default values are necessary for this command.

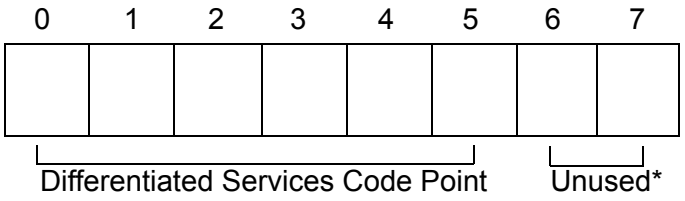
Command History

Release 11.1	Command was introduced.

Functional Notes

The differentiated services (DiffServ or DS) model was created in RFC 2474 and RFC 2475 to build on the original type of service (ToS) field by creating a six-bit sequence (combining the precedence value with the delay, throughput, and reliability bits). This six-bit sequence increased the number of available values from 8 to 64. The DiffServ model introduced a new concept to quality of service (QoS) in the IP network environment: per-hop behaviors (PHBs). The PHB premise is that equipment using the DiffServ model have an agreed upon set of rules (PHB types) for handling certain network traffic. Though the RFC explicitly defines what each PHB should be capable of, it does not restrict vendor-specific implementation of the PHBs. Each vendor is free to decide how their network product implements the various defined PHBs.

According to RFC 2474, the DS field contains the following bits:



* The previously unused bits in the DS field are now used for congestion control and are not discussed in this document.

Equipment following the DiffServ model (DS-compliant nodes) must use the entire six-bit DSCP value to determine the appropriate PHB. The PHBs are defined as the following:

- Default PHB
- Class selector PHB
- Assured forwarding PHB (RFC 2597)
- Expedited forwarding PHB (RFC 2598)

Default PHB

All DS-compliant nodes must provide a default PHB to offer best-effort forwarding service. For default PHBs, the DSCP value is 0. Any packet that does not contain a standardized DSCP should be mapped to the Default PHB and handled accordingly.

Class Selector PHB

In the class selector PHB, the first three bits in the DSCP value are used for backwards compatibility to systems implementing IP precedence. In this scenario, all but the first three bits of the DS field are set to 0. This compatibility requires DS-compliant nodes to provide the same data services as are provided by nodes implementing IP precedence. The following table is a comparison of IP precedence values to their corresponding DSCP values.

IP Precedence Value (bits)	DSCP Value (bits)
0 (000)	0 (000000)
1 (001)	8 (001000)
2 (010)	16 (010000)
3 (011)	24 (011000)
4 (100)	32 (100000)
5 (101)	40 (101000)
6 (110)	48 (110000)
7 (111)	56 (111000)

Assured Forwarding PHB

The flexibility of DiffServ allows for more developed subclasses of service within each main class using the last three bits of the DSCP. As defined in RFC 2597, the assured forwarding PHB creates four main classes of service:

Class	DSCP Bits
AF1	001XX0
AF2	010XX0
AF3	011XX0
AF4	100XX0
X indicates a do not care value.	

The first three bits of the DSCP specify the class and the last bit is always zero. Each class is separated into subclasses using the two remaining bits in the DSCP (bits 3 and 4). The subclasses are divided based on the likelihood that packets in the class are dropped in the event of network congestion. The higher the value for bits 3 and 4, the greater the likelihood that the packets will be dropped.

Bit 3	Bit 4	Drop Precedence
0	1	Low
1	0	Medium
1	1	High

The following table lists the assured forwarding PHB subclasses and their corresponding DSCP bits and values.

Class	Subclass	DSCP Bits	DSCP Value
AF1	1	001010	10
	2	001100	12
	3	001110	14
AF2	1	010010	18
	2	010100	20
	3	010110	22
AF3	1	011010	26
	2	011100	28
	3	011110	30
AF4	1	100010	34
	2	100100	36
	3	100110	38

Expedited Forwarding PHB

RFC 2598 created a new DiffServ PHB intended to provide the best service possible on an IP network. Packets using the expedited forwarding PHB markings should provide service to reduce latency, jitter, and dropped packets, and be guaranteed bandwidth during the entire end-to-end transmission journey through the network. The DSCP value for the expedited forwarding PHB is 46 (DSCP bits are 101110).

Usage Examples

The following example instructs the route map named **MYMAP** to match the IP header with a DSCP AF Class 1, Subclass 2 (**af12**):

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match ip dscp af12**

match ip precedence

Use the **match ip precedence** command to configure the route map to route traffic based on the precedence value in the IP header of the packet. Use the **no** form of this command to discontinue matching. Variations of this command include:

match ip precedence <*value*>
match ip precedence critical
match ip precedence flash
match ip precedence flash-override
match ip precedence immediate
match ip precedence internet
match ip precedence network
match ip precedence priority
match ip precedence routine

Syntax Description

<*value*>	Specifies matching the IP precedence (in numeric value). Valid range is **0** to **7** in ascending order of importance.
routine	Specifies matching the IP precedence **routine**. (Numeric value of 0.)
priority	Specifies matching the IP precedence **priority**. (Numeric value of 1.)
immediate	Specifies matching the IP precedence **immediate**. (Numeric value of 2.)
flash	Specifies matching the IP precedence **flash**. (Numeric value of 3.)
flash-override	Specifies matching the IP precedence **flash-override**. (Numeric value of 4.)
critical	Specifies matching the IP precedence **critical**. (Numeric value of 5.)
internet	Specifies matching the IP precedence **internet**. (Numeric value of 6.) This level is reserved for internal network use.
network	Specifies matching the IP precedence **network**. (Numeric value of 7.) This level is reserved for internal network use.

Default Values

No default values are necessary for this command.

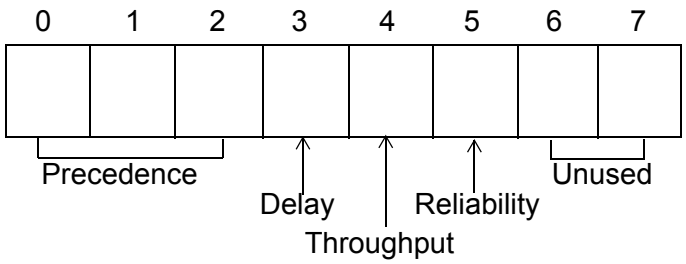
Command History

Release 11.1	Command was introduced.

Functional Notes

RFC 791 created a single octet (labeled type of service (ToS)) to help with the difficulty of trying to provide quality of service (QoS) handling in IP networks.

According to RFC 791, the ToS field contains the following bits:



The three-bit IP precedence values (0 through 7) are specified as:

111	Network Control Packets
110	Internetwork Control Packets
101	Critical Traffic
100	Flash Override
011	Flash
010	Immediate Servicing
001	Priority Traffic
000	Routine Data

The IP precedence values provide network routers with information about the kind of traffic contained in the IP packet. Based on the IP precedence values, some networks (when supported) can offer special handling to certain packets. In addition, providing IP precedence values to critical traffic (such as route information) ensures that critical packets will always be delivered regardless of network congestion. This traffic is often critical to network and internetwork operation. In general, the higher the IP precedence value, the more important the traffic and the better handling it should receive in the network. It is important to remember that not all equipment in the public IP network will be configured to recognize and handle IP precedence values. While it is a good idea to set the values for critical traffic, it does not guarantee special handling.

In addition to the IP precedence values, RFC 791 specifies bits for delay, throughput, and reliability to help balance the needs of particular traffic types when traveling on the IP network infrastructure. When these bits are set to 0, they are handled with normal operation. When set to 1, each bit specifies premium handling for that parameter. For example, a 1 in the delay position indicates that the traffic is delay sensitive and care should be taken to minimize delay. A 1 in the throughput position indicates that the traffic has higher bandwidth requirements that should be met. A 1 in the reliability position indicates that the traffic is sensitive to delivery issues and care should be taken to ensure proper delivery with all packets of this type. These extra bits are rarely used because it is quite difficult to balance the cost and benefits of each parameter (especially when more than one bit is set to 1).

Usage Examples

The following example instructs the route map named **MyMap** to match the IP precedence value of **critical**:

(config)**#route-map MyMap permit 100**
(config-route-map)**#match ip precedence critical**

match ipv6 address *<ipv6 acl name>*

Use the **match ipv6 address** command to configure the route map to route traffic based on the Internet Protocol version 6 (IPv6) access control list (ACL) name defined with the **ipv6 access-list** command. Refer to *ipv6 access-list standard <ipv6 acl name> on page 1502* for more information. Use the **no** form of this command to discontinue matching.

Syntax Description

<ipv6 acl name>	Specifies the name of the IPv6 ACL to match.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match the IPv6 address ACL named **MYLIST**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match ipv6 address MYLIST**

match ipv6 address prefix-list *<name>*

Use the **match ipv6 address prefix-list** command to configure the route map to route traffic based on an Internet Protocol version 6 (IPv6) prefix list route filter. The name of the prefix list is defined with the command *ipv6 prefix-list <name> seq <number> on page 1556*. Use the **no** form of this command to discontinue matching.

Syntax Description

<name>	Specifies matching the IPv6 address based on the IPv6 prefix list name.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match the IPv6 address prefix list named **MYLIST**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match ipv6 address prefix-list MYLIST**

match length *<minimum> <maximum>*

Use the **match length** command to configure the route map to route traffic based on the packet length. Use the **no** form of this command to discontinue matching.

Syntax Description

<minimum>	Specifies the minimum packet length you want to match. Valid range is **1** to **4294967295**.
<maximum>	Specifies the maximum packet length you want to match. Valid range is **1** to **4294967295**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match packets with a minimum length of **1** and a maximum length of **200**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match length 1 200**

match metric <*value*>

Use the **match metric** command to configure the route map to route traffic based on a specified metric value. Use the **no** form of this command to discontinue matching.

Syntax Description

<*value*>	Specifies the metric value you want to match. Valid range is **1** to **4294967295**.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to match the metric value **100**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match metric 100**

match tag <*number*>

Use the **match tag** command to configure the route map to filter traffic based on a route's tag value. Use the **no** form of this command to discontinue matching.

match tag <*number*>
match tag <*number*> <*number*>

Syntax Description

<*number*>	Specifies the desired route tag value to match. If more than one value is specified, the match command will pass if any value matches. Valid range is **1** to **65535**.

Default Values

No default values are necessary for this command.

Command History

Release 15.1	Command was introduced.

Functional Notes

More than one value may be specified as a tag to be matched.

Usage Examples

The following example instructs the route map named **MYMAP** to match a route tag of 100 or 200:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#match tag 100 200**

Technical Review

The command *ip route on page 1447* is related to the **match tag** command in that it includes an optional parameter to set the route tag value for local static routes.

Virtual private network (VPN) reverse-route injection (RRI) routes can also have a tag applied.

set as-path prepend

Use the **set as-path prepend** command to prepend a number to the autonomous system (AS) path to influence the best-path selection process by making the AS path appear further away. Use the **no** form of this command to disable this feature. Variations of this command include:

set as-path prepend <*number*>
set as-path prepend last-as <*number*>

Syntax Description

<*number*>	Specifies a number to be prepended to the AS path value as an autonomous number. Valid range is **1** to **65535**.
last-as <*number*>	Specifies a number to be prepended to the last AS path number. Valid range is **1** to **10**.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example prepends the number **2** to the last AS path number:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set as-path prepend last-as 2**

set comm-list <*name*> delete

Use the **set comm-list delete** command to specify a list of communities to delete. Use the **no** form of this command to disable this feature.

Syntax Description

<name>	Specifies the name of the IP community list that contains the list of community strings to delete.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

A community list must be defined using the **ip community-list** command before the **set comm-list delete** command can be used. Refer to *community-list <name> on page 1236* for information on configuring a community list.

Usage Examples

The following example deletes the community list named **LISTNAME**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set comm-list LISTNAME delete**

set community

Use the **set community** command to modify the community attribute for all paths serviced by the route map. Use the **no** form of this command to disable this feature. Variations of this command include:

set community <*value*>
set community <*value*> **add**
set community <*value*> **internet**
set community <*value*> **local-as**
set community <*value*> **no-advertise**
set community <*value*> **no-export**
set community none

Syntax Description

<*value*>	Sets the community attribute to the specified community number for routes serviced by this route map. This is a numeric value that can be an integer from **1** to **4294967295** or string in the form ***aa:nn***, where the value of ***aa*** is the autonomous system (AS) number and the value of ***nn*** is the community number. Multiple community-number parameters can be present in the command.
add	Appends the listed community number to the end of the community attribute for routes serviced by this route map.
internet	Sets the community attribute to the INTERNET community number for routes serviced by this route map.
local-as	Sets the community attribute to the NO_EXPORT_SUBCONFED community number for routes serviced by this route map. Routes containing this attribute should not be advertised to external Border Gateway Protocol (BGP) peers.
no-advertise	Sets the community attribute to the NO_ADVERTISE community number for routes serviced by this route map. Routes containing this attribute should not be advertised to any BGP peer.
no-export	Sets the community attribute to the NO_EXPORT community number for routes serviced by this route map. Routes containing this attribute should not be advertised to BGP peers outside a confederation boundary.
none	Removes all communities from BGP routes serviced by this route map.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the community number for BGP routes to the Internet community:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set community internet**

set default interface

Use the **set default interface** command to specify a default interface to redirect traffic to the specified interface if there is no specific routing information for the traffic. If more than one interface is specified, the router uses the first available interface from the list. Use the **no** form of this command to remove the default interface. Variations of this command include:

set default interface <*interface*>
set default interface efm-group <*slot/port.subint*>
set default interface null 0

Syntax Description

<*interface*>	Specifies the default interface. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **set default interface ?** for a list of valid interface types.
efm-group <*slot/port.subint*>	Specifies an Ethernet in the first mile (EFM) group interface. Interface number is specified in <*slot/port.subinterface id*>.
null 0	Redirects traffic to the specified interface regardless of available routing information.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release R11.2.0	Command was expanded to include Ethernet in the first mile (EFM) group.
Release R11.4.0	Command was expanded to include the Gigabit Ethernet interface.
Release R13.7.0	Command was expanded to include the VLAN interface.

Usage Examples

The following example sets the default interface as **ppp 1** interface:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set default interface ppp 1**

set interface <*interface*>

Use the **set interface** command to specify an output interface for the packet. Multiple interfaces can be specified. The router forwards the packet along the first usable interface. Use the **no** form of this command to cancel output from the specified interface. Variations of this command include:

set interface <*interface*>
set interface efm-group <*slot/port.subint*>

Syntax Description

<*interface*>	Sets output interface type for the packet. Specify an interface in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **set interface ?** for a list of valid interfaces.
efm-group <*slot/port.subint*>	Specifies an Ethernet in the first mile (EFM) group interface. Interface number is specified in <*slot/port.subinterface id*>.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release R11.2.0	Command was expanded to include Ethernet in the first mile (EFM) group.
Release R11.4.0	Command was expanded to include the Gigabit Ethernet interface.
Release R13.7.0	Command was expanded to include the VLAN interface.

Usage Examples

The following example sets the output interface as Point-to-Point Protocol (PPP) 1:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set interface ppp 1**

set ip default next-hop *<interface>*

Use the **set ip default next-hop** command to set the next-hop IP address to the specified interface's address for all routes serviced by the route map that do not have explicit routing information available. Use the **no** form of this command to remove the configured default next hop.

Syntax Description

<interface>	Specifies the default interface. Specify an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **set default next-hop ?** for a list of valid interface types.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the default next-hop interface to the **ppp 1** interface:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set ip default next-hop ppp 1**

set ip df

Use the **set ip df** command to identify the packet as *don't fragment* (DF). Use the **no** form of this command to remove this designation.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example designates the packet as DF:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set ip df**

set ip dscp

Use the **set ip dscp** command to configure the route map to set the differentiated services code point (DSCP) value in the IP header of the packet for traffic serviced by this route map. For more details on DSCP values, refer to the command *match ip dscp on page 4174*. Use the **no** form of this command to remove the specified DSCP value. Variations of this command include:

set ip dscp <*value*>
set ip dscp af*xx*
set ip dscp cs*x*
set ip dscp default
set ip dscp ef

Syntax Description

<*value*>	Specifies the DSCP numeric value. Valid range is **0** to **63**.
af*xx*	Specifies the assured forwarding (AF) class and subclass. Select from: 11 (001010), 12 (001100), 13 (001110), 21 (010010), 22 (010100), 23 (010110), 31 (011010), 32 (011100), 33 (011110), 41 (100010), 42 (100100), or 43 (100110).
cs*x*	Specifies the class selector (CS) value. Valid range is **1** to **7**.
default	Specifies the default IP DSCP value (000000).
ef	Specifies marking for expedited forwarding (EF).

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MYMAP** to set the IP header with a DSCP AF Class 1, Subclass 2 (**af12**):

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set ip dscp af12**

set ip next-hop *<ip address>*

Use the **set ip next-hop** command to set the next-hop IP address to the specified address for all routes serviced by the route map. Use the **no** form of this command to remove the configured next-hop address.

Syntax Description

<ip address>	Specifies a valid IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). More than one address can be entered, and the router uses the first available route from the list.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the ip next-hop interface to **10.10.11.254** in the header of the route map named **MYMAP**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set ip next-hop 10.10.11.254**

set ip precedence

Use the **set ip precedence** command to configure the route map to set the precedence value in the IP header of the packet for traffic serviced by the route map. For more details on IP precedence values, refer to the command *match ip precedence on page 4178*. Use the **no** form of this command to remove the specified IP precedence value. Variations of this command include:

set ip precedence <*value*>
set ip precedence critical
set ip precedence flash
set ip precedence flash-override
set ip precedence immediate
set ip precedence internet
set ip precedence network
set ip precedence priority
set ip precedence routine

Syntax Description

<*value*>	Specifies matching the IP precedence (in numeric value). Valid range is **0** to **7** in ascending order of importance.
routine	Specifies matching the IP precedence **routine**. (Numeric value of 0.)
priority	Specifies matching the IP precedence **priority**. (Numeric value of 1.)
immediate	Specifies matching the IP precedence **immediate**. (Numeric value of 2.)
flash	Specifies matching the IP precedence **flash**. (Numeric value of 3.)
flash-override	Specifies matching the IP precedence **flash-override**. (Numeric value of 4.)
critical	Specifies matching the IP precedence **critical**. (Numeric value of 5.)
internet	Specifies matching the IP precedence **internet**. (Numeric value of 6.) This level is reserved for internal network use.
network	Specifies matching the IP precedence **network**. (Numeric value of 7.) This level is reserved for internal network use.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets an IP precedence value of **critical** in the IP header of the route map named **MYMAP**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set ip precedence critical**

set ipv6 next-hop <*ipv6 address*>

Use the **set ipv6 next-hop** command to set the next-hop Internet Protocol version 6 (IPv6) address to the specified address for all routes serviced by the route map. Use the **no** form of this command to remove the configured next-hop address.

Syntax Description

<ipv6 address>	Specifies a valid IPv6 address. IPv6 addresses should be expressed in colon hexadecimal notation (**X:X:X:X::X**), for example, **2001:DB8:1::1**. More than one address can be entered, and the router uses the first available route from the list.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example sets the IPv6 address of the next hop to **2001:DB8:1::1** in the header of the route map named **MYMAP**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set ipv6 next-hop 2001:DB8:1::1**

set local-preference *<value>*

Use the **set local-preference** command to restrict traffic to a local autonomous system (AS). Use the **no** form of this command to cancel the local preference.

Syntax Description

<value>	Sets the local preference value. Valid range is **0** to **4294967295**.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the local preference for **MYMAP** to a value of **100**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set local-preference 100**

set metric *<value>*

Use the **set metric** command to specify a metric value for the route map. Use the **no** form of this command to cancel the metric value.

Syntax Description

<value>	Sets the metric value. Valid range is **0** to **4294967295**.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the metric value for **MYMAP** to **100**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set metric 100**

set metric-type

Use the **set metric-type** command to set the open shortest path first (OSPF) metric type for the route map. Use the **no** form of this command to return to the default value. Variations of this command include:

set metric-type type-1
set metric-type type-2

Syntax Description

type-1	Specifies intra-area metric.
type-2	Specifies inter-area metric.

Default Values

By default, the metric type is set to **type 1**.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example sets the metric-type value for **MYMAP** to **type 2**:

(config)**#route-map MYMAP permit 100**
(config-route-map)**#set metric-type type-2**

set tag <*value*>

Use the **set tag** command to set the open shortest path first (OSPF) route tag for the route map. This command applies the specified route tag to any route matched by the route map. Use the **no** form of this command to cancel the route tag.

Syntax Description

<*value*>	Specifies the route tag value. Valid range is **0** to **4294967295**.

Default Values

By default, no route tag is set.

Command History

Release R11.4.0	Command was introduced.

Usage Examples

The following example sets the route tag value for **OSPFMAP** to **555**:

(config)**#route-map OSPFMAP permit 100**
(config-route-map)**#set tag 555**

ROUTER PIM SPARSE COMMAND SET

To activate the Router (Protocol-Independent Multicast (PIM) Sparse) Configuration mode, enter the **router pim-sparse** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router pim-sparse
(config-pim-sparse)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

join-prune-msg-interval <value> on page 4202
rp-address <ip address> on page 4203
spt-threshold on page 4204

join-prune-msg-interval <*value*>

Use the **join-prune-msg-interval** command to set a timing rate for protocol-independent multicast (PIM) sparse join/prune messages. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the PIM sparse join/prune message interval. Valid range: **10** to **65534** seconds.

Default Values

By default, the message interval is set to **60** seconds.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the interval for **50** seconds:

(config)**#router pim-sparse**
(config-pim-sparse)**#join-prune-msg-interval 50**

rp-address <*ip address*>

Use the **rp-address** command to specify a static IP address for the rendezvous point (RP) router. The **access-group** keyword is used to limit the multicast group addresses to which the RP applies. Use the **no** form of this command to remove a static IP address for the RP router. Variations of this command include:

rp-address <*ip address*>
rp-address <*ip address*> **access-group** <*name*>

Syntax Description

<*ip address*>	Specifies the IP address for the RP. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
access-group <*name*>	Optional. Specifies the particular access group to which the RP applies.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Functional Notes

The **access-group** keyword is used to limit the multicast group addresses to which the RP applies. If more than one RP is configured for a given multicast group address, then a hash algorithm determines the appropriate hierarchy (as shown below). The results of the hash algorithm can be seen with the **show ip pim-sparse rp-map** command.

The hash algorithm is defined in RFC 2117 section 3.7 as follows:

For each RP address C(i) in the RP-Set, whose Group-prefix covers G, compute a value:

Value(G,M,C(i))=(1103515245 * ((1103515245 * (G&M)+12345) XOR C(i)) + 12345) mod 2^31

where M is a hash-mask included in Bootstrap messages.This hash-mask allows a small number of consecutive groups (e.g., **4**) to always hash to the same RP. For instance, hierarchically encoded data can be sent on consecutive group addresses to get the same delay and fate-sharing characteristics.

The candidate with the highest resulting value is then chosen as the RP for that group, and its identity and hash value are stored with the entry created.

Ties between C-RPs having the same hash value are broken in advantage of the highest address.

Usage Examples

The following example specifies an IP address of **172.22.5.100** for the RP:

(config)**#router pim-sparse**
(config-pim-sparse)**#rp-address 172.22.5.100**

spt-threshold

Use the **spt-threshold** command to change the protocol-independent multicast (PIM) sparse shortest path tree (SPT) threshold, which specifies the number of packets the router sends using the rendezvous point (RP) before switching to the SPT. Use the **no** form of this command to return to the default setting. Variations of this command include:

spt-threshold <*value*>
spt-threshold infinity

Syntax Description

<*value*>	Optional. Specifies the number of packets the routing switch sends using the RP before switching to the SPT. Valid range is **1** to **4294967295** packets.
infinity	Optional. Causes all sources to use the shared RP tree.

Default Values

By default, the SPT threshold is set to **1** packet.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the SPT threshold at **five** packets:

(config)**#router pim-sparse**
(config-pim-sparse)**#spt-threshold 5**

ROUTER RIP COMMAND SET

To activate the Router (Routing Information Protocol (RIP)) Configuration mode, enter the **router rip** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router rip
(config-rip)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

auto-summary on page 4206
default-metric <value> on page 4207
distance <number> on page 4208
distribute-list <name> on page 4209
network <ip address> <subnet mask> on page 4211
passive-interface <interface> on page 4212
redistribute bgp on page 4213
redistribute connected on page 4214
redistribute ospf on page 4215
redistribute static on page 4217
timeout-timer <value> on page 4218
update-timer <value> on page 4219
version on page 4220

auto-summary

Use the **auto-summary** command to have Routing Information Protocol (RIP) version 2 summarize subnets to the classful boundaries. Use the **no** form of this command to disable this summarization.

Syntax Description

No subcommands.

Default Values

By default, **auto-summary** is disabled.

Command History

Release 3.1	Command was introduced.

Functional Notes

Use this command if you are subdividing a classful network into many subnets and these subnets are to be advertised over a slow link (64k or less) to a router that can only reach the classful network via the router you are configuring.

Usage Examples

The following example configures the router to not automatically summarize network numbers:

(config)**#router rip**
(config-rip)**#no auto-summary**

default-metric *<value>*

Use the **default-metric** command to set the default metric value for the Routing Information Protocol (RIP). Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Sets the default metric value in Mbps. Range is **1** to **4294967295** Mbps.

Default Values

By default, this value is set at **0**.

Command History

Release 3.1	Command was introduced.

Functional Notes

The metric value defined using the **redistribute** command overrides the **default-metric** command's metric setting. Refer to *redistribute ospf on page 4215* for related information.

Usage Examples

The following example shows a router using both RIP and open shortest path first (OSPF) routing protocols. The example advertises OSPF-derived routes using RIP and assigns the OSPF-derived routes a RIP metric of **10**.

(config)**#router rip**
(config-rip)**#default-metric 10**
(config-rip)**#redistribute ospf**

distance <*number*>

Use the **distance** command to set the administrative distance for Routing Information Protocol (RIP) routes that are added to the route table. Use the **no** form of this command to set the RIP administrative distance to the default value.

Syntax Description

<*number*>	Specifies the new administrative distance. Range is **0** to **255**.

Default Values

By default, the administrative distance for RIP routes is set to **120**.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following configuration sets the administrative distance to **109**, which gives RIP routes a lower administrative distance than open shortest path first (OSPF) routes:

(config)**#router rip**
(config-rip)**#distance 109**

Technical Review

Administrative distance is a feature that routers employ in order to select the most reliable path when there are two or more routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol by assigning a value (the smaller the value, the more trustworthy the protocol) that is then used by the router to organize routing protocols according to reliability.

distribute-list <*name*>

Use the **distribute-list** command to add route filtering functionality by assigning inbound and outbound access control lists (ACLs) on either a per-interface or global basis. Only one inbound/outbound pair of ACLs can be configured for a particular interface. Use the **no** form of this command to disable the filtering. Variations of this command include:

distribute-list <*name*> **in**
distribute-list <*name*> **in** <*interface*>
distribute-list <*name*> **out**
distribute-list <*name*> **out** <*info source*>

Syntax Description

<*name*>	Specifies an ACL name. This is a standard IP ACL against which the contents of the incoming/outgoing routing updates are matched.
in	Applies route filtering to inbound data.
in <*interface*>	Optional. Specifies the interface in which to apply the ACL. Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id* | *ap* | *ap/radio* | *ap/radio.vap]*>. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **distribute-list list1 in ?** for a complete list of applicable interfaces.
out	Applies route filtering to outbound data.
out <*info source*>	Optional. Specifies the source of the routing information. The source can be an interface or a routing process (**connected**, **ospf**, **rip**, or **static**). Type **distribute list** <*name*> **out ?** for a list of available options.

Default Values

By default, distribute-list filtering is disabled.

Command History

Release 12.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release A5.01	Command was epxanded to include the Gigabit Ethernet interface.

Usage Examples

The following example filters out all network advertisements received via Ethernet interface **0/1** with the exception of the **10.10.10.0** network:

(config)**#router rip**
(config-rip)**#version 2**
(config-rip)**#network 192.168.1.0 255.255.255.0**
(config-rip)**#distribute-list list_1 in eth 0/1**
(config-rip)**#exit**
(config)**#ip access-list standard list_1**
(config-std-nacl)**#permit 10.10.10.0 0.0.0.255**

network *<ip address> <subnet mask>*

Use the **network** command to enable Routing Information Protocol (RIP) on the specified network. Use the **no** form of this command to remove a network from the list.

Syntax Description

<ip address>	Specifies the IP address of the network on which RIP will be enabled. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IP addresses (network). Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**).

Default Values

By default, RIP is not enabled.

Command History

Release 1.1	Command was introduced.

Functional Notes

AOS will only allow processing (sending and receiving) RIP messages on interfaces with IP addresses that are contained in the networks listed using this command. All RIP messages received on interfaces not listed using this command will be discarded. To allow for receiving and participating in RIP, but not for transmitting, use the **passive-interface** command (refer to *passive-interface <interface> on page 4212*).

Usage Examples

The following example enables RIP on the **102.22.72.252 /30**, **192.45.2.0 /24**, and **10.200.0.0 /16** networks:

(config)**#router rip**
(config-rip)**#network 102.22.72.252 255.255.255.252**
(config-rip)**#network 192.45.2.0 255.255.255.0**
(config-rip)**#network 10.200.0.0 255.255.0.0**

passive-interface *<interface>*

Use the **passive-interface** command to disable the transmission of routing updates on the specified interface. Use the **no** form of this command to enable the transmission of routing updates on an interface.

Syntax Description

<interface>	Specifies an interface in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id | ap | ap/radio | ap/radio.vap]>*. For example, for a T1 interface, use **t1 0/1**; for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; for an ATM subinterface, use **atm 1.1**; and for a wireless virtual access point, use **dot11ap 1/1.1**. Type **passive-interface ?** for a complete list of valid interfaces.

Default Values

By default, Routing Information Protocol (RIP) is not enabled.

Command History

Release 1.1	Command was introduced.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

All routing updates received on that interface will still be processed (and advertised to other interfaces), but no updates will be transmitted to the network connected to the specified interface. Multiple **passive-interface** commands may be used to create a customized list of interfaces.

Usage Examples

The following example disables routing updates on the Frame Relay link (labeled **1.17**) and the Point-to-Point Protocol (PPP) link (labeled **1**):

(config)**#router rip**
(config-rip)**#passive-interface frame-relay 1.17**
(config-rip)**#passive-interface ppp 1**

redistribute bgp

Use the **redistribute bgp** command to redistribute routes from one protocol to another, regardless of the routing protocol implemented on the routing domain. Using the **bgp** keyword allows the propagation of Border Gateway Protocol (BGP) routes into Routing Information Protocol (RIP). Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute bgp
redistribute bgp metric <*value*>
redistribute bgp route-map <*name*>

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed BGP routes in RIP.
route-map <*name*>	Optional. Specifies the route map filter to use for advertising redistributed BGP routes in RIP.

Default Values

By default, this command is disabled.

Command History

Release 14.1	Command was introduced.

Functional Notes

Redistributing BGP routes imports those routes into RIP without the interfaces in question actually participating in RIP. The BGP routes imported this way are not covered by a network command and are learned via BGP. This allows RIP to distribute routes for networks that are not participating in this RIP network.

If **redistribute bgp** is enabled and no metric value is specified, the value defaults to **0**. The metric value defined using the **redistribute bgp metric** command overrides the **default-metric** command's metric setting. Refer to *default-metric <value> on page 4207* for more information.

Usage Examples

The following example imports BGP routes into RIP:

(config)**#router rip**
(config-rip)**#redistribute bgp**

redistribute connected

Use the **redistribute connected** command to pass routes from one network to another, regardless of the routing protocol implemented on the routing domain. Using the **connected** keyword allows the propagation of routes connected to other interfaces using the Routing Information Protocol (RIP). Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute connected
redistribute connected metric <*value*>
redistribute connected route-map <*name*>

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed routes in RIP.
route-map <*name*>	Optional. Specifies the route map filter to use for advertising redistributed routes in RIP.

Default Values

By default, this command is disabled.

Command History

Release 3.1	Command was introduced.
Release 14.1	Command was expanded to include the route map filtering.

Functional Notes

Redistributing connected routes imports those routes into RIP without the interfaces in question actually participating in RIP. The connected routes imported this way are not covered by a network command and do not send/receive RIP traffic.

Usage Examples

The following example passes the connected routes found in the route table to other networks running the RIP routing protocol:

(config)**#router rip**
(config-rip)**#redistribute connected**

redistribute ospf

Use the **redistribute ospf** command to redistribute routes from one protocol to another, regardless of the routing protocol implemented on the routing domain. Using the **ospf** keyword allows the propagation of open shortest path first (OSPF) routes into Routing Information Protocol (RIP). Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute ospf
redistribute ospf <*process id*>
redistribute ospf <*process id*> **metric** <*value*>
redistribute ospf <*process id*> **no-include-connected**
redistribute ospf <*process id*> **route-map** <*name*>

After specifying the process id, the other parameters can be entered in any order. Use the ***?*** *after each specified subcommand for a valid list of arguments and settings.*

Syntax Description

<*process id*>	Optional. Specifies the OSPFv2 routing process from which RIP routes will be redistributed. The process ID is locally significant to the device, and must be unique among OSPFv2 processes on the device. Valid range is **1** to **65535**.
metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed OSPF routes in RIP.
no-include-connected	Optional. Specifies that prefixes of the interface running this source protocol are not automatically included in the route redistribution.
route-map <*name*>	Optional. Specifies the route map filter to use for advertising redistributed OSPF routes in RIP.

Default Values

By default, this command is disabled.

Command History

Release 3.1	Command was introduced.
Release 14.1	Command was expanded to include the route map filtering.
Release R11.3.0	Command was expanded to include the <*process id*> and **no-include-connected** parameters.

Functional Notes

Redistributing OSPF routes imports those routes into RIP without the interfaces in question actually participating in RIP. The OSPF routes imported this way are not covered by a network command and do not send/receive RIP traffic. This allows RIP to distribute routes for networks that are not participating in this RIP network.

If **redistribute ospf** is enabled and no metric value is specified, the value defaults to **0**. The metric value defined using the **redistribute ospf metric** command overrides the **default-metric** command's metric setting. Refer to *default-metric <value> on page 4207* for more information.

Usage Examples

The following example imports OSPF routes into RIP:

(config)**#router rip**
(config-rip)**#redistribute ospf**

redistribute static

Use the **redistribute static** command to pass routes from one network to another, regardless of the routing protocol implemented on the routing domain. Using the **static** keyword allows the propagation of static routes to other interfaces using the Routing Information Protocol (RIP). Use the **no** form of this command to disable the propagation of the specified route type. Variations of this command include:

redistribute static
redistribute static metric <*value*>
redistribute static route-map <*name*>

The gateway network for the static route must participate in RIP by using the network command for the gateway network.

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed static routes in RIP.
route-map <*name*>	Optional. Specifies the route map filter to use for advertising redistributed static routes in RIP.

Default Values

By default, this command is disabled.

Command History

Release 1.1	Command was introduced.
Release 14.1	Command was expanded to include the route map filtering.

Functional Notes

Redistributing static routes allows other network devices to learn about routes without requiring manual input to each device on the network.

Usage Examples

The following example passes the static routes found in the route table to other networks running the RIP routing protocol:

(config)**#router rip**
(config-rip)**#redistribute static**

timeout-timer <*value*>

Use the **timeout-timer** command to set the timeout timer value for a route when it is learned via Routing Information Protocol (RIP). Each time a RIP update for that route is received, the timeout timer is reset to this value. If no updates for that route are received in the specified number of seconds and the timeout timer expires, the route is considered invalid, and it will be removed from the route table. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Sets the timeout timer value. Valid range is **5** to **4294967295** seconds.

Default Values

By default, this value is set at **180** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Note that the timeout timer value cannot be set to a value less than the **update-timer** value. It is recommended that this timer be set to a value that is three times the value of the **update-timer** (refer to *update-timer <value> on page 4219*).

Usage Examples

The following example configures the router to mark routes invalid if no RIP updates for those routes are received within **120** seconds:

(config)**#router rip**
(config-rip)**#timeout-timer 120**

update-timer <*value*>

Use the **update-timer** command to set the value of the Routing Information Protocol (RIP) update interval timer. The RIP update interval is the number of seconds that must elapse between RIP update packet transmissions. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the number of seconds allowed to elapse between RIP update packet transmissions. Valid range is **5** to **4294967295** seconds.

Default Values

By default, this value is set at **30** seconds.

Command History

Release 11.1	Command was introduced.

Functional Notes

Note that the **timeout-timer** value cannot be set to a value less than the **update-timer** value. It is recommended that the **timeout-timer** be set to a value that is three times the value of the **update-timer**. (Refer to *timeout-timer <value> on page 4218* for more information.)

Usage Examples

The following example sets the rate at which RIP update messages are transmitted from the router to **20** seconds.

(config)**#router rip**
(config-rip)**#update-timer 20**

version

Use the **version** command to specify (globally) the Routing Information Protocol (RIP) version used on all IP interfaces. This global configuration is overridden using the configuration commands **ip rip send version** and **ip rip receive version**. Use the **no** form of this command to return to the default value. Variations of this command include:

version 1
version 2

Syntax Description

1	Specifies RIP version **1** be used globally.
2	Specifies RIP version **2** be used globally.

Default Values

By default, RIP is not enabled.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies RIP version **2** as the global RIP version:

(config)**#router rip**
(config-rip)**#version 2**

VRRPv3 Command Set

Virtual Router Redundancy Protocol version 3 (VRRPv3) is a standard protocol that allows multiple physical routers to act as a single virtual router on an Ethernet network. The virtual router is comprised of two or more physical routers running VRRPv3, and acts as a single virtual router for hosts on a shared local area network (LAN). This functionality provides seamless redundancy to networked end-host devices, and allows the forwarding of host traffic if a router or interface port fails within the network. VRRPv3 is defined in RFC 3768, and functions similarly to IPv4 VRRPv2, with the primary difference being the support of both IPv4 and IPv6. For more information about the implementation of VRRPv3, refer to the configuration guide *VRRPv3 in AOS*, available online at https://supportcommunity.adtran.com.

To enable VRRPv3, and enter the virtual router instance's configuration mode, enter the **vrrpv3** <*vrid*> **address-family [ipv4 | ipv6]** command from the interface's configuration mode. For example, to enable VRRPv3, create a virtual router ID of **15**, and specify VRRPv3 with IPv6, enter the command as follows:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#vrrpv3 15 address-family ipv6
(config-if-vrrpv3 15)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

address <ipv4 address> on page 4222
address <ipv6 address> on page 4223
description <text> on page 4225
match-address on page 4226
preempt on page 4227
priority <level> on page 4228
startup-delay <delay> on page 4229
timers advertise <interval> on page 4230
track <name> on page 4231

address *<ipv4 address>*

Use the **address** *<ipv4 address>* command to assign an IPv4 address to the virtual router. Using the **no** form of this command removes the address from the virtual router's configuration. Variations of this command include:

address *<ipv4 address>*
address *<ipv4 address>* **primary**
address *<ipv4 address>* **secondary**

Syntax Description

<ipv4 address>	Specifies the IPv4 address for the virtual router. IPv4 addresses should be expressed in decimal dotted notation, for example, **10.10.10.1**, and must include a subnet mask.
primary	Specifies the IPv4 address is the primary address for the virtual router.
secondary	Specifies the IPv4 address is the secondary address for the virtual router.

Default Values

By default, no IPv4 addresses are assigned to the virtual router instance.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

This command is for use with IPv4 VRRPv3.

The primary address must be configured before the virtual router will become active, and before any secondary addresses can be added. The primary address is the only address that can be an owner address (the configured router IPv4 address for the interface).

Usage Examples

The following example creates an IPv4 virtual router instance with an assigned address of **10.10.10.1 255.255.255.0**:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#address 10.10.10.1 255.255.255.0 primary**

address *<ipv6 address>*

Use the **address** *<ipv6 link-local address>* command to assign a link-local IPv6 address to the virtual router. Use the **no** form of this command to remove the IPv6 address from the virtual router. Variations of this command include:

address *<ipv6 link-local address>* **primary**
address generate primary
address *<ipv6 global-address>* **secondary**

Syntax Description

<ipv6 link-local address>	Specifies the link-local address to assign to the virtual router. A link-local IPv6 address is specified in the format **FE80::**<*bits*>. The <*bits*> are the lower 64 bits of the link-local IPv6 address, and since link-local addresses have no prefix, the bits entered form the entire IPv6 address.
primary	Specifies this is the primary IPv6 address for the virtual router.
generate primary	Optional. Specifies that a default virtual link-local address is assigned to the virtual router. Default link-local addresses are created based on a computation from the virtual interface ID (VRID) and the virtual medium access control (MAC) address associated with the VRID.
<ipv6 global-address>	Specifies the IPv6 global address to assign to the virtual router. Specify IPv6 addresses in colon hexadecimal format, for example, **2001:DB8::1**.
secondary	Specifies the address is the IPv6 global address.

Default Values

By default, no IPv6 addresses are assigned to the virtual router instance.

Command History

Release R10.11.0	Command was introduced. This command replaces the **vrrpv3** <*number*> **link-local** command on the interface.

Functional Notes

This command is for use with IPv6 VRRPv3. IPv6 must be enabled on the interface before IPv6 VRRPv3 can be configured.

A virtual link-local address must be configured before the VRRPv3 router becomes active. Only one virtual link-local address can be specified per virtual router. The IPv6 global address can be specified using the **secondary** keyword with the *<ipv6 global-address>* parameter.

Usage Examples

The following example creates an IPv6 virtual router instance with an assigned default link-local address:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6**
(config-eth 0/1)**#vrrpv3 15 address-family ipv6**
(config-if-vrrpv3 15)**#address generate primary**

description *<text>*

Use the **description** command to add a text description to the Virtual Router Redundancy Protocol version 3 (VRRPv3) group. Use the **no** form of this command to remove the description from the virtual router's configuration.

Syntax Description

<text>	Specifies the text string used to describe the virtual router instance.

Default Values

By default, no text description of the virtual router exists.

Command History

Release R10.11.0	Command was introduced. This command replaces the **vrrpv3** *<number>* **description** *<text>* command on the interface.

Usage Examples

The following example adds a description to the virtual router instance:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#description RemoteRoutersA**

match-address

Use the **match-address** command to specify that IPv4 or IPv6 Virtual Router Redundancy Protocol version 3 (VRRPv3) virtual routers will match secondary IP addresses when receiving packets from nearby virtual routers. Use the **no** form of this command to disable secondary address matching.

Syntax Description

No subcommands.

Default Values

By default, secondary address matching is enabled for VRRPv3.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

This command is available for both IPv4 and IPv6 VRRPv3.

Secondary address matching is used to verify configuration consistency between neighboring virtual routers. Primary address matching is always enforced, regardless of whether secondary address matching is enabled.

Usage Examples

The following example enables secondary address matching for the virtual router:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#match-address**

preempt

Use the **preempt** command to specify that a virtual router can preempt the current master router. Use the **no** form of this command to disable preemption. Variations of this command include:

preempt
preempt delay minimum <*delay*>

Syntax Description

delay minimum <*delay*>	Optional. Specifies that the router waits a specified amount of time before attempting to preempt the master router. Valid range is **0** to **255** seconds.

Default Values

By default, a virtual router preempts with no additional delay.

Command History

Release R10.11.0	Command was introduced. This command replaces the **vrrpv3** <*number*> **preempt** command on the interface.

Functional Notes

Whenever a Virtual Router Redundancy Protocol version 3 (VRRPv3) router with a higher actual priority level than the current master is added to a virtual router group, it attempts to take over or preempt the master router if preemption is enabled. This behavior may be desired, for example, when the new router is more powerful than the existing master router.

When VRRPv3 transitions occur between master and backup devices, security related configurations can be affected and security policies may need to be adjusted. For example, preemption might need to be disabled to prevent loss of state or session, particularly in use of long-term Transmission Control Protocol (TCP) connections, such as Telnet or Secure Socket Layer (SSL).

Using the **no** form of this command disables preemption, unless the master router is the link-local address owner, in which case it will always preempt, and this command is ignored.

Usage Examples

The following example enables a preempt after **30** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#preempt delay minimum 30**

priority <*level*>

Use the **priority** command to specify the virtual router instance priority. Use the **no** form of this command to return the virtual router priority to the default value.

Syntax Description

<*level*>	Specifies the configured priority level for the virtual router. Valid range is **1** to **254**.

Default Values

By default, the virtual router's priority is **100**, unless it is the owner of the virtual link-local address, in which case the priority default is **255**.

Command History

Release R10.11.0	Command was introduced. This command replaces the **vrrpv3** <*number*> **priority** <*level*> command on the interface.

Functional Notes

It is possible for VRRPv3 to operate based on default priority level settings. However, it is important to understand and verify the election process to ensure the desired VRRPv3 router is ultimately selected as the master. The virtual router master is selected using an election process based on the priority level setting of each VRRPv3 router. There are two types of priority levels: configured and actual. The configured priority level is the numerical value originally assigned to the VRRPv3 router. The actual priority level is a value that takes into account any adjustments resulting from a track event. The VRRPv3 router with the highest actual priority level is the virtual router master. If there is a tie, the actual priority level will be used along with the interface link-local address to determine the master.

If the virtual link-local address of the virtual router is the same as the interface address on the VRRPv3 router (the link-local address owner), then the default priority level will be **255**. This is the highest priority level and means that when the link-local address owner is available, it will be the virtual router master.

Usage Examples

The following example configures a virtual router priority of **200**:

(config)**#interface eth 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#priority 200**

startup-delay <*delay*>

Use the **startup-delay** command to specify that the virtual router waits a specified amount of time before running the Virtual Router Redundancy Protocol version 3 (VRRPv3) state machine after initial activation. Use the **no** form of this command to return to the default value.

Syntax Description

<*delay*>	Specifies the delay (in seconds) that the virtual router waits to run VRRPv3. Valid range is **0** to **255** seconds.

Default Values

By default, the startup delay is set to **35** seconds.

Command History

Release R10.11.0	Command was introduced. This command replaces the **vrrpv3** <*number*> **startup-delay** <*delay*> command on the interface.

Functional Notes

Startup delay can prevent inadvertent declarations of multiple VRRPv3 masters while waiting for potentially slower interfaces to begin passing advertisement traffic.

If the virtual router receives an advertisement from an external master during the delay period, it assumes that the network path is open, cancels the timer, and transitions to the appropriate backup or master state.

Usage Examples

The following example creates a virtual router with a startup delay of **100** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#startup-delay 100**

timers advertise <*interval*>

Use the **timers advertise** command to specify the interval between Virtual Router Redundancy Protocol version 3 (VRRPv3) advertisements sent by the master router. Use the **no** form of this command to return the advertisement interval to the default value.

Syntax Description

<*interval*>	Specifies the time, in seconds, between sent advertisements. Valid range is **1** to **40** seconds.

Default Values

By default, advertisements are sent every **1** second.

Command History

Release R10.11.0	Command was introduced. This command replaces the **vrrpv3** <*number*> **timers advertise** <*interval*> command on the interface.

Functional Notes

All VRRPv3 routers in a virtual router group must use the same advertisement interval.

Usage Examples

The following example changes the advertisement interval to **5** seconds:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#timers advertise 5**

track <*name*>

Use the **track** command to track objects associated with the virtual router. Use the **no** form of this command to remove the track reference and its configuration from the virtual router. Variations of this command include:

track <*name*>
track <*name*> **decrement** <*value*>

Syntax Description

<*name*>	Specifies the name of the track to apply to the virtual router.
decrement <*value*>	Optional. Specifies the amount to decrement the router's priority level if the track transitions to a FAIL state. Valid range is **1** to **254**.

Default Values

By default, tracks are not associated with virtual routers. If a track is associated with a virtual router, its priority decrements by **10** if the track transitions to a FAIL state.

Command History

Release R10.11.0	Command was introduced. This command replaces the **vrrpv3** <*number*> **track** <*name*> command on the interface.

Functional Notes

Object tracking can be used to change the priority level of a VRRPv3 router. One purpose of object tracking for VRRPv3 is to detect failure of the interface or main path connected to the master router. The object that is tracked is typically an interface towards the far end of the main path. Depending on the object type specified, as long as the line protocol for the interface is up, the track will remain in a PASS state and nothing will change. However, if the line protocol for an interface goes down, the track will transition to a FAIL state. This transition will cause the priority level of the VRRPv3 router to be decremented by the numerical amount specified (or the default amount).

If a VRRPv3 router owns the virtual router link-local address, then the VRRPv3 router's priority level cannot be decremented as a result of the **track** command. Therefore, if object tracking is used to monitor paths and effectively decrement priority levels in case of interface or path failure, then it is important that no VRRPv3 router own the virtual router link-local address.

A track must be created before this command can be used. For detailed information about creating tracks, refer to the configuration guide *Configuring Network Monitor in AOS*, available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the virtual router is associated with **TRACK1** and will decrement its priority by **20** if the track changes to a FAIL state:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#vrrpv3 15 address-family ipv4**
(config-if-vrrpv3 15)**#track TRACK1 decrement 20**

SECURITY AND SERVICES COMMAND SETS

The security and services command sets are divided into the following sections:

ACCESS CONTROL LISTS AND ACCESS CONTROL POLICIES COMMAND SETS

This section includes the following command sets:

HARDWARE ACL AND ACCESS MAP COMMAND SET

Hardware access control lists (ACLs) are access lists that function by comparing incoming frames to specific criteria at the hardware level. These hardware ACLs function in the same way typical IP ACLs do at the software level. The difference is that hardware ACLs filter incoming traffic through the switch chip at wire speeds, rather than through software packet filtering processes.

It is beneficial to understand the basic functioning of ACLs in AOS before working with hardware ACLs. All ACLs, whether hardware or software, by themselves do not perform any action. Rather, they are lists of criteria to which all incoming frames are compared. These lists provide the methods for many of the configurable filtering and security features of AOS to logically inspect each frame, compare it to the criteria in the ACL, and behave accordingly.

ACLs list criteria for incoming frames that begin with either the keyword **permit** or **deny**. **Permit** indicates that frames matching the specific criteria are selected and handled according to the configuration of the AOS feature using the ACL. **Deny** indicates that frames matching the specific criteria are not selected and are handled accordingly. Each ACL's criteria are compared to the frame in the order in which it was entered. This means that the order of criteria for permitting or denying frames is one to one with the order in which the criteria were entered into the ACL's configuration. As frames come into the unit, they are compared to the ACL criteria from top-to-bottom. If a frame does not match the criteria specified by the first entry, then it is compared to the criteria in the next entry. When the frame is found to match an entry's specified criteria, then the frame is either categorized as **permit** or **deny** and the comparison of the ACL entries abruptly stops. At this point, the feature using the ACL takes the appropriate action.

There are many uses for ACLs, and many ways to configure ACLs. If you would like more information about ACL basic configuration and uses in AOS, refer to the configuration guide *Hardware ACLs in AOS* available online at https://supportcommunity.adtran.com. Specific commands for configuring ACLs are also included in this guide in the section *IPv4 Access Control List Command Set on page 4252*.

Hardware ACLs and Hardware Access Maps

Hardware ACLs can filter frames based either on IP information or on medium access control (MAC) address information. IP hardware ACLs support filtering traffic on source and destination IP addresses, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and TCP or UDP port numbers. MAC hardware ACLs filter traffic based on source and destination MAC addresses. All hardware ACLs filter only the incoming traffic, comparing the traffic to the list of criteria cited in the ACL.

As with all ACLs, the hardware ACL by itself performs no action. In order for the hardware ACL to function, a hardware access map must be created and applied to a virtual local area network (VLAN) interface. Access maps are the feature that uses the ACL and performs the action on the incoming traffic. Each access map can either forward or discard incoming frames acting on a single IP hardware ACL, a single MAC hardware ACL, or both. When both an IP and MAC hardware ACL are used by the access map, the two ACLs are linked by **and** logic. **And** logic indicates to the access map that *both* ACLs must conclude that the frame be forwarded for the access map to forward it. As with all other ACLs, the information entered into the hardware ACLs is order dependent. The order in which criteria is listed in the ACL configuration is the order in which the frames will be compared to the criteria.

Once the access map has been created and associated with a hardware ACL, it must be applied to a virtual local area network (VLAN) for the ACL to be fully functional. Access maps can be applied to a single VLAN or a range of VLANs, however, only one access map can be applied to a VLAN at a time.

To create an IP hardware ACL and enter the ACL's configuration, enter the command *ip hw-access-list extended <name> on page 1404* from the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip hw-access-list extended Trusted
        Configuring New IP Hardware Extended ACL "Trusted"
(config-ext-ip-hw-nacl)#
```

TTo create an extended MAC hardware ACL and enter the ACL's configuration, enter the command **mac hw-access-list extended** <*name*> from the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#mac hw-access-list extended Untrusted
        Configuring New MAC Hardware Extended ACL "Untrusted"
(config-ext-mac-hw-nacl)#
```

To create a standard MAC hardware ACL and enter the ACL's configuration, enter the command **mac hw-access-list standard** <*name*> from the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#mac hw-access-list standard Untrusted
        Configuring New MAC Hardware Standard ACL "Untrusted"
(config-std-mac-hw-nacl)#
```

To create a hardware access map and enter the map's configuration, enter the command *hw-access-map <name> on page 1337* from the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#hw-access-map Map1
(config-hw-access-map)#
```

Technology Review

Hardware access maps and ACLs regulate traffic through the routed network. When designing your traffic flow configuration, it is important to keep the following in mind:

- A hardware ACL serves as a traffic selector, defining exactly which frames should take the given action.
- A hardware access map defines the action to take on the frames selected by the ACL.
- A hardware ACL is inactive until it is assigned to an active hardware access map.

- A hardware access map is inactive until it is assigned to a VLAN interface.

> NOTE *For more information on both hardware ACLs and hardware access maps, refer to the Hardware ACLs in AOS configuration guide available online at* https://supportcommunity.adtran.com.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76

The following are commands used to configure an **IP** hardware ACL. **IP** hardware ACL configuration includes creating a remark for the ACL, specifying an ACL action, a protocol, a packet source, a source port, a packet destination, and a destination port. These commands are described in this section in alphabetical order:

deny <protocol> <source> <source port> <destination> <destination port> on page 4238
permit <protocol> <source> <source port> <destination> <destination port> on page 4240
remark <text> on page 4242

The following are commands used to configure an extended or standard **MAC** hardware ACL. **MAC** hardware ACL configuration includes creating a remark for the ACL, specifying the ACL action, a source MAC address, and a destination MAC address. These commands are described in this section in alphabetical order:

deny mac <source> <destination> on page 4243
permit mac <source> <destination> on page 4245
remark <text> on page 4242

The following are commands used to configure a hardware access map. Access map configuration includes specifying which hardware ACL(s) the map will use and the relationship between those ACLs, and applying the access map to a VLAN or VLANs. These commands are described in this section in alphabetical order:

forward ip <acl name> on page 4247
forward mac <acl name> on page 4249
vlans <vlan id> on page 4251

deny *<protocol> <source> <source port> <destination> <destination port>*

Use the **deny** command to configure the IP hardware access control list (ACL) to deny specified packets to enter the system. Use the **no** form of this command to remove the deny parameter from the ACL. Variations of this command include:

deny *<protocol> <source> <source port> <destination> <destination port>*
deny *<protocol> <source> <source port> <destination> <destination port>* **log**

Syntax Description

<protocol>	Specifies the data protocol as **ip**, **tcp**, or **udp**.	
<source>	Specifies the source used for packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IP address. 2. Using **host** *<ip address>* to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). 3. Using the *<ip address> <wildcard mask>* format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).	
<source port>	Optional. The source port is used only when *<protocol>* is **tcp** or **udp**. The following keywords and port numbers/names are supported for the *<source port>* field:	
	eq *<port>*	Matches only packets equal to the specified port number. Range is **0** to **65535**.
	range *<min> <max>*	Matches only packets that contain a port number in the specified range. Range is **0** to **65535**.
<destination>	Specifies the destination used for packet matching. Destinations can be expressed in one of three ways: 1. Using the keyword **any** to match any IP address. 2. Using **host** *<ip address>* to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). 3. Using the *<ip address> <wildcard mask>* format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).	
<destination port>	Optional. The destination port is used only when *<protocol>* is **tcp** or **udp**. The following keywords and port numbers are supported for the *<destination port>* field:	
	eq *<port>*	Matches only packets equal to the specified port number. Range is **0** to **65535**.

	range <*min*> <*max*>	Matches only packets that contain a port number in the specified range. Range is **0** to **65535**.
log		Optional. Enables logging of any packets that match the hardware ACL entry.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware ACLs.

Command History

Release 17.6	Command was introduced.

Functional Notes

Hardware ACLs are used as frame selectors by the hardware access maps; by themselves they do nothing. Hardware ACLs are composed of an ordered list of entries with an implicit **deny any** at the end of each list. A hardware ACL with no entries includes an implicit **permit any**. An ACL entry contains two parts: an action (**permit** or **deny**) and a frame pattern. A **permit** ACL matches frames (meeting the specified pattern) and allows them to enter the network. A **deny** ACL advances AOS to the next ACL entry.

ACL criteria are compared to the incoming frame in the order in which they were entered or from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

Usage Examples

The following example creates an IP hardware ACL **Untrusted** to deny packets from any source destined for IP address **192.168.20.0**:

(config)**#ip hw-access-list extended Untrusted**
(config-ext-ip-hw-nacl)**#deny ip any host 192.168.20.0**

The following example creates an entry in the **Untrusted** IP hardware ACL that denies any UDP packets from being forwarded to the UDP ports that range between **1080** and **1150**:

(config)**#ip hw-access-list extended Untrusted**
(config-ext-nacl)**#deny udp any any range 1080 1150**

permit *<protocol> <source> <source port> <destination> <destination port>*

Use the **permit** command to configure the IP hardware access control list (ACL) to permit specified packets to enter the system. Use the **no** form of this command to remove the permit parameter from the ACL. Variations of this command include:

permit <*protocol*> <*source*> <*source port*> <*destination*> <*destination port*>
permit <*protocol*> <*source*> <*source port*> <*destination*> <*destination port*> **log**

Syntax Description

<*protocol*>	Specifies the data protocol as **ip**, **tcp**, or **udp**.	
<*source*>	Specifies the source used for packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IP address. 2. Using **host** <*ip address*> to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). 3. Using the <*ip address*> <*wildcard mask*> format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).	
<*source port*>	Optional. The source port is used only when <*protocol*> is **tcp** or **udp**. The following keywords and port numbers/names are supported for the <*source port*> field:	
	eq <*port*>	Matches only packets equal to the specified port number. Range is **0** to **65535**.
	range <*min*> <*max*>	Matches only packets that contain a port number in the specified range. Range is **0** to **65535**.
<*destination*>	Specifies the destination used for packet matching. Destinations can be expressed in one of three ways: 1. Using the keyword **any** to match any IP address. 2. Using **host** <*ip address*> to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). 3. Using the <*ip address*> <*wildcard mask*> format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).	
<*destination port*>	Optional. The destination port is used only when <*protocol*> is **tcp** or **udp**. The following keywords and port numbers are supported for the <*destination port*> field:	
	eq <*port*>	Matches only packets equal to the specified port number. Range is **0** to **65535**.

	range <*min*> <*max*>	Matches only packets that contain a port number in the specified range. Range is **0** to **65535**.
log		Optional. Enables logging of any packets that match the hardware ACL entry.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware ACLs.

Command History

Release 17.6	Command was introduced.

Functional Notes

Hardware ACLs are used as frame selectors by the hardware access maps; by themselves they do nothing. Hardware ACLs are composed of an ordered list of entries with an implicit **deny any** at the end of each list. A hardware ACL with no entries includes an implicit **permit any**. An ACL entry contains two parts: an action (**permit** or **deny**) and a frame pattern. A **permit** ACL matches frames (meeting the specified pattern) and allows them to enter the network. A **deny** ACL advances AOS to the next ACL entry.

ACL criteria are compared to the incoming frame in the order in which they were entered or from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

Usage Examples

The following example creates an IP hardware ACL **Trusted** to permit packets from any source destined for IP address **192.168.20.0**:

(config)**#ip hw-access-list extended Trusted**
(config-ext-ip-hw-nacl)**#permit ip any host 192.168.20.0**

The following example creates an entry in the **Trusted** IP hardware ACL that permits any UDP packets to be forwarded to the UDP ports that range between **1080** and **1150**:

(config)**#ip hw-access-list extended Trusted**
(config-ext-nacl)**#permit udp any any range 1080 1150**

remark *<text>*

Use the **remark** command to associate a descriptive tag with a hardware access control list (ACL). Use the **no** form of this command to remove the descriptive tag.

Syntax Description

<text>	Specifies a descriptive tag for the ACL. Tags can be up to **80** alphanumeric characters. For example, **This list blocks all outbound Web traffic**.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware ACLs.

Command History

Release 17.6	Command was introduced.
Release R11.5.0	Command was expanded to include standard medium access control (MAC) ACLs.

Usage Examples

The following example specifies a description for IP hardware ACL **Matchall**:

(config)**#ip hw-access-list extended Matchall**
(config-ext-ip-hw-nacl)**#remark Allows all IP traffic from remote location.**

The following example specifies a description for an extended MAC hardware ACL **Matchall**:

(config)**#mac hw-access-list extended Matchall**
(config-ext-mac-hw-nacl)**#remark Allows all IP traffic from remote location.**

deny mac *<source> <destination>*

Use the **deny mac** command to configure the standard or extended medium access control (MAC) hardware access control list (ACL) to deny specified frames to enter the system. Use the **no** form of this command to remove the deny parameters from the ACL. Variations of this command include:

deny mac <*source*>
deny mac <*source*> <*destination*>
deny mac <*source*> <*destination*> **log**

Syntax Description

<*source*>	Specifies the source used for frame matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any MAC address. 2. Using **address** <*mac address*> to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **08:00:69:02:06:CB**). 3. Using the <*mac address*> <*wildcard mask*> format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
<*destination*>	Applies only to extended MAC ACLs. Specifies the destination used for frame matching. Destinations can be expressed in one of three ways: 1. Using the keyword **any** to match any MAC address. 2. Using **address** <*mac address*> to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **08:00:69:02:06:CB**). 3. Using the <*mac address*> <*wildcard mask*> format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
log	Optional. Enables logging of any frames that match the hardware ACL entry.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware ACLs.

Command History

Release 17.6	Command was introduced.
Release R11.5.0	Command was expanded to include standard MAC ACLs.

Functional Notes

Hardware ACLs are used as frame selectors by the hardware access maps; by themselves they do nothing. Hardware ACLs are composed of an ordered list of entries with an implicit **deny any** at the end of each list. A hardware ACL with no entries includes an implicit **permit any**. An ACL entry contains two parts: an action (**permit** or **deny**) and a frame pattern. A **permit** ACL matches frames (meeting the specified pattern) and allows them to enter the network. A **deny** ACL advances AOS to the next access list entry.

ACL criteria are compared to the incoming frame in the order in which they were entered or from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

Usage Examples

The following example specifies that the extended MAC hardware ACL **Untrusted** deny traffic from MAC address **08:00:69:02:01:FC** with a destination of MAC address **08:00:69:02:06:CB**. Traffic that matches this description will be logged.

(config)**#mac hw-access-list extended Untrusted**
(config-ext-mac-hw-nacl)**#deny address 08:00:69:02:01:FC address 08:00:69:02:06:CB log**

permit mac *<source> <destination>*

Use the **permit mac** command to configure the extended or standard medium access control (MAC) hardware access control list (ACL) to permit specified frames to enter the system. Use the **no** form of this command to remove the permit parameters from the ACL. Variations of this command include:

permit mac <*source*>
permit mac <*source*> <*destination*>
permit mac <*source*> <*destination*> **log**

Syntax Description

<*source*>	Specifies the source used for frame matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any MAC address. 2. Using **address** <*mac address*> to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **08:00:69:02:06:CB**). 3. Using the <*mac address*> <*wildcard mask*> format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
<*destination*>	Applies only to extended MAC ACLs. Specifies the destination used for frame matching. Destinations can be expressed in one of three ways: 1. Using the keyword **any** to match any MAC address. 2. Using **address** <*mac address*> to specify a single host address. IP addresses should be expressed in dotted decimal notation (for example, **08:00:69:02:06:CB**). 3. Using the <*mac address*> <*wildcard mask*> format to match all IP addresses in a range. The wildcard mask corresponds to a range of IP addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
log	Optional. Enables logging of any frames that match the hardware ACL entry.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware ACLs.

Command History

Release 17.6	Command was introduced.
Release R11.5.0	Command was expanded to include standard MAC ACLs.

Functional Notes

Hardware ACLs are used as frame selectors by the hardware access maps; by themselves they do nothing. Hardware ACLs are composed of an ordered list of entries with an implicit **deny any** at the end of each list. A hardware ACL with no entries includes an implicit **permit any**. An ACL entry contains two parts: an action (**permit** or **deny**) and a frame pattern. A **permit** ACL matches frames (meeting the specified pattern) and allows them to enter the network. A **deny** ACL advances AOS to the next access list entry.

ACL criteria are compared to the incoming frame in the order in which they were entered or from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

Usage Examples

The following example specifies that the extended MAC hardware ACL **Trusted** permit traffic from any MAC address destined for MAC address **08:00:69:02:06:CB**. Traffic that matches this description will be logged.

(config)**#mac hw-access-list extended Trusted**
(config-ext-mac-hw-nacl)**#permit any address 08:00:69:02:06:CB log**

forward ip <*acl name*>

Use the **forward ip** command to specify which IP hardware access control list (ACL) the hardware access map will use to determine which frames to forward. Use the **no** form of this command removes this action from the access map. Variations of this command include:

forward ip <*acl name*>
forward ip <*acl name*> **and mac** <*acl name*>

Syntax Description

<*acl name*>	Specifies the hardware ACL the access map will use when determining which traffic to forward.
mac <*acl name*>	Specifies the medium access control (MAC) hardware ACL that the access map will use in conjunction with the IP hardware ACL to determine which traffic to forward.
and	Specifies that the relationship between the IP and MAC ACLs is such that the access map will forward traffic only if both ACLs indicate that it should be forwarded.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware access maps.

Command History

Release 17.6	Command was introduced.

Functional Notes

Hardware access maps can only forward traffic. This action can be performed based on the criteria outlined in a single IP hardware ACL, a single MAC hardware ACL, or both. Like the hardware ACLs, the hardware access map will match traffic in top-down order. Use the **forward ip** command if the first criteria for the access map is to match traffic based on IP information.

Specifying **and** indicates to the access map that both ACLs must conclude the frame should be forwarded for the access map to forward it.

If you configure the access map to reference a nonexistent IP or MAC hardware ACL, the ACL will be created. Note that this newly created ACL will have **permit any** as the default entry because no other entries are present.

Hardware access maps are not active until they are applied to a virtual local area network (VLAN). For instructions on how to apply an access map to a VLAN, refer to *vlans <vlan id> on page 4251*.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

Usage Examples

In the following example, the access map **Map1** is configured to operate on both an IP hardware ACL (**Trusted)** and a MAC hardware ACL (**Untrusted**), specifying that both must agree that a frame should be forwarded before the access list will forward it.

(config)**#hw-access-map Map1**
(config-hw-access-map)**#forward ip Trusted and mac Untrusted**

forward mac *<acl name>*

Use the **forward mac** command to specify which medium access control (MAC) hardware access control list (ACL) the hardware access map will use to determine which frames to forward. Use the **no** form of this command removes this action from the access map. Variations of this command include:

forward mac *<acl name>*
forward mac *<acl name>* **and ip** *<acl name>*

Syntax Description

<acl name>	Specifies the hardware ACL the access map will use when determining which traffic to forward.
ip *<acl name>*	Specifies the IP hardware ACL that the access map will use in conjunction with the MAC hardware ACL to determine which traffic to forward.
and	Specifies that the relationship between the MAC and IP ACLs is such that the access map will forward traffic only if both ACLs indicate that it should be forwarded.

Default Values

By default, all AOS security features are disabled, and there are no configured hardware access maps.

Command History

Release 17.6	Command was introduced.

Functional Notes

Hardware access maps can only forward traffic. This action can be performed based on the criteria outlined in a single IP hardware ACL, a single MAC hardware ACL, or both. Like the hardware ACLs, the hardware access map will match traffic in top-down order. Use the **forward mac** command if the first criteria for the access map is to match traffic based on MAC addresses.

Specifying **and** indicates to the access map that both ACLs must conclude the frame should be forwarded for the access map to forward it.

If you configure the access map to reference a nonexistent IP or MAC hardware ACL, the ACL will be created. Note that this newly created ACL will have **permit any** as the default entry because no other entries are present.

Hardware access maps are not active until they are applied to a virtual local area network (VLAN). For instructions on how to apply an access map to a VLAN, refer to *vlans <vlan id> on page 4251*.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command show hw-filter-resource on page 672.

Usage Examples

In the following example, the access map **Map1** is configured to operate on both a MAC hardware ACL (**Trusted)** and an IP hardware ACL (**Untrusted**), specifying that both must agree that a frame should be forwarded before the access list will forward it.

(config)**#hw-access-map Map1**
(config-hw-access-map)**#forward mac Trusted and ip Untrusted**

vlans <*vlan id*>

Use the **vlans** command to apply a hardware access map to a virtual local area network (VLAN) interface. Access maps can be applied to a single VLAN, a list of VLANs, or a range of VLANs. Use the **no** form of this command to remove the access map from the specified VLAN(s).

Syntax Description

<vlan id>	Specifies the VLAN(s) to which the access map is applied. Enter the single VLAN ID for the map to apply to a single VLAN. Enter multiple VLAN IDs separated by commas to apply the map to a list of VLANs (for example: **1,2,7,9**). Enter multiple VLANs separated by dashes or commas to apply the map to a range of VLANs (for example: **1-5,7-9**).

Default Values

By default, access maps are not applied to any VLAN interfaces.

Command History

Release 17.6	Command was introduced.

Functional Notes

Once an access map has been created and associated with a hardware access control list (ACL), it must be applied to a VLAN for the ACL or access map to be fully functional. Access maps can be applied to a single VLAN or a range of VLANs, however, only one access map can be applied to a VLAN at a time. If you attempt to apply a second access map to a VLAN, an error is displayed.

Changing hardware ACL or hardware access map configuration or application causes new information to be reinstalled on the hardware. It is possible to run out of hardware resources depending on how many resources are needed to apply the desired change. If there are not enough hardware resources to install the new criteria in the hardware, an error message is displayed. You can view the amount of hardware resources available using the command *show hw-filter-resource on page 672*.

Usage Examples

The following example specifies that the access map **Map1**, which uses IP hardware ACL **Trusted** and **MAC** hardware ACL **Untrusted**, is applied to VLANs **1**,**2**, and **15-30**.

(config)**#hw-access-map Map1**
(config-hw-access-map)**#forward ip Trusted and mac Untrusted**
(config-hw-access-map)**#vlans 1,2,15-30**

IPv4 Access Control List Command Set

An Internet Protocol version 4 (IPv4) access control list (ACL) is an ordered list of entries used as packet selectors by an IPv4 access control policy (ACP) in the Adtran Operating System (AOS) command line interface (CLI). ACLs and ACPs work together to regulate IPv4 traffic through the routed network.

There are two types of IPv4 ACLs within AOS: **standard** and **extended**. A **standard** IPv4 ACL allows source IPv4 address packet patterns only. An **extended** IPv4 ACL may specify patterns using most fields in the IPv4 header and the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) header. This configuration command set details the configuration of both a standard and an extended IPv4 ACL.

IPv6 ACLs are also supported by AOS, but are explained separately in this document. Refer to IPv6 Access Control List Command Set on page 4296 for more information on configuring IPv6 ACLs.

To create a **standard** IPv4 ACL and activate the Standard IPv4 ACL Configuration mode, enter the **ip access-list standard** <*name*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip access-list standard MATCHALL
(config-std-nacl)#
```

To create an **extended** IPv4 ACL and activate the Extended IPv4 ACL Configuration Mode, enter the **ip access-list extended** <*name*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip access-list extended MATCHALL
(config-ext-nacl)#
```

*An IPv4 ACL will remain inactive until it is assigned to an **active** IPv4 ACP. For more information on configuring and activating IPv4 ACPs, refer to the IPv4 Access Control Policy Command Set on page 4278.*

Technology Review

IPv4 ACPs and IPv4 ACLs regulate traffic through the routed network. When designing your traffic flow configuration, it is important to keep the following in mind:

- An IPv4 ACL serves as a packet selector, defining exactly which packets should take the given action.
- An IPv4 ACP defines the action to take on the packets selected by the ACL.
- An IPv4 ACL is inactive until it is assigned to an active ACP.
- An IPv4 ACP is inactive until it is assigned to an interface.

IPv4 Access Control Policies (ACPs)

IPv4 ACPs are used to allow, discard, or manipulate (using network address translation (NAT)) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (IPv4 ACL). In a sense, the IPv4 ACPs answer the question, “What should I do?” while the IPv4 ACLs answer the question, “On which packets?”

When packets are received on an interface with an IPv4 ACP applied, the ACP is used to determine whether the data is processed or discarded. Both IPv4 ACLs and IPv4 ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed. The IPv4 ACP has an implicit **discard** at the end of the list. Typically, the most specific entries should be at the top and the most general at the bottom.

IPv4 Access Control Lists (ACLs)

IPv4 ACLs are used as packet selectors by IPv4 ACPs. They must be assigned to an IPv4 ACP in order to be active.

IPv4 ACP must use an IPv4 ACL. You cannot apply an IPv4 ACL to an IPv6 ACP, or vice-versa. In addition, all IPv4 ACLs and IPv4 ACPs must have a different name than any configured IPv6 ACLs or IPv6 ACPs.

IPv4 ACLs are composed of an ordered list of entries. Each entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** action is used to allow packets (meeting the specified pattern) to enter the router system. A **deny** action is used to disregard packets (that do not match the pattern) and proceed to the next entry on the IPv4 ACP. The IPv4 ACL has an implicit **deny** at the end of the list.

The AOS provides two types of IPv4 ACLs: **standard** and **extended**. A **standard** IPv4 ACL allows source IPv4 address packet patterns only. An **extended** IPv4 ACL may specify patterns using most fields in the IPv4 header and the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) header.

Creating and Assigning IPv4 ACLs and IPv4 ACPs

Creating IPv4 ACPs and IPv4 ACLs to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of AOS using the **ip firewall** command. Refer to the command *ip firewall on page 1367* for more information.

Step 2:
Create an IPv4 ACP that uses a configured IPv4 ACL by issuing the **ip policy-class** command. AOS IPv4 ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (IPv4 ACL). When packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

Step 3:
Create an IPv4 ACL to permit or deny specified traffic by using either the **ip access-list extended** or **ip access-list standard** command. Standard IPv4 ACLs match based on the source IPv4 address of the packet. Extended IPv4 ACLs match based on the source and destination of the packet. Refer to the command *ip access-list extended <ipv4 acl name> on page 1344* or the command *ip access-list standard <ipv4 acl name> on page 1346* for more information. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IPv4 address.

2. Using **host** *<ipv4 address>* to specify a single host address.

3. Using the *<ipv4 address>* *<wildcard>* format to match all IPv4 addresses in a range. Wildcard masks work in reverse logic from subnet masks. When broken out into binary form, a 0 indicates which bits of the IPv4 address to consider, a 1 indicates which bits are disregarded. For example, specifying 255 in any octet of the wildcard mask equates to a “don’t care” for that octet in the IPv4 address. Additionally, a 30-bit mask would be represented with the wildcard string 0.0.0.3, a 28-bit mask with 0.0.0.15, a 24-bit mask with 0.0.0.255, and so forth.

4. Using the keyword **hostname** to match based on a domain naming system (DNS) name. DNS servers must be configured or host names must be locally defined for this function to work.

Step 4:
Apply the created IPv4 ACP to an interface. To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** *<ipv4 acp name>*. The following example assigns ACP **UNTRUSTED** to the Ethernet 0/1 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip access-policy UNTRUSTED**

For more information about configuring ACLs, ACPs, and the AOS Firewall, refer to the IPv4 Firewall configuration guide available at https://supportcommunity.adtran.com.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

The following are commands used to configure an **extended** IPv4 ACL. **Extended** IPv4 ACL configuration includes specifying an IPv4 ACL action, a protocol, a packet source, a source port, a packet destination, and a destination port. These commands are described in this section in alphabetical order.

deny <protocol> <source> <source port> <destination> <destination port> on page 4256
deny icmp <source> <destination> on page 4260

The following are commands for configuring a **standard** IPv4 ACL. **Standard** IPv4 ACL configuration includes specifying an IPv4 ACL action and a packet source. These commands are described in this section in alphabetical order.

deny *<protocol> <source> <source port> <destination> <destination port>*

Use the **deny** command to configure the Internet Protocol version 4 (IPv4) extended access control list (ACL) to deny specified packets entry into the routing system. Use the **no** form of this command to remove the deny parameter from the ACL. Variations of this command include:

deny *<protocol> <source> <source port> <destination> <destination port>*
deny *<protocol> <source> <source port> <destination> <destination port>* **log**
deny *<protocol> <source> <source port> <destination> <destination port>* **track** *<name>*
deny ip *<source> <source port> <destination> <destination port>* **fragments**

Syntax Description

<protocol> Specifies the data protocol **ip**, **tcp**, **udp**, **ahp**, **esp**, **gre**, or a specific protocol. Range is **0** to **255**.

<source> Specifies the source used for packet matching. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** *<ip address>* to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the *<ip address> <wildcard mask>* format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** *<hostname>* to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** *<name>* in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<source port> Optional. The source port is used only when *<protocol>* is **tcp** or **udp**. The following keywords and port numbers/names are supported for the *<source port>* field:

any	Matches any destination port.
eq *<port number/name>*	Matches only packets equal to specified port number.
gt *<port number/name>*	Matches only packets with a port number greater than the specified port number.
lt *<port number/name>*	Matches only packets with a port number less than the specified port number.
neq *<port number/name>*	Matches only packets that are not equal to the specified port number.
range *<begin port number/name> <end port number/name>*	Matches only packets that contain a port number in the specified range.

<port number>	Specifies the port number used by Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) to pass information to upper layers using the following syntax: <***0-65535***>. All ports below 1024 are considered well-known ports, and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above 1024 are dynamically assigned ports that include registered ports for vendor-specific applications.
<port name>	The following UDP port numbers can be specified using the associated names: **biff** (Port 512) **bootpc** (Port 68) **bootps** (Port 67) **discard** (Port 9) **dnsix** (Port 195) **domain** (Port 53) **echo** (Port 7) **isakmp** (Port 500) **mobile-ip** (Port 434) **nameserver** (Port 42) **netbios-dgm** (Port 138) **netbios-ns** (Port 137) **netbios-ss** (Port 139) **ntp** (Port 123) **pim-auto-rp** (Port 496) **rip** (Port 520) **snmp** (Port 161) **snmptrap** (Port 162) **sunrpc** (Port 111) **syslog** (Port 514) **tacacs** (Port 49) **talk** (Port 517) **tftp** (Port 69) **time** (Port 37) **who** (Port 513) **xdmcp** (Port 177) The following TCP port numbers can be specified using the associated names: **bgp** (Port 179) **chargen** (Port 19) **cmd** (Port 514) **daytime** (Port 13) **discard** (Port 9) **domain** (Port 53) **echo** (Port 7) **exec** (Port 512) **finger** (Port 79) **ftp** (Port 21) **gopher** (Port 70) **hostname** (Port 101) **ident** (Port 113) **lpd** (Port 515) **nntp** (Port 119) **pim-auto-rp** (Port 496) **pop2** (Port 109) **pop3** (Port 110) **smtp** (Port 25) **sunrpc** (Port 111) **tacacs** (Port 49) **talk** (Port 517) **tftp** (Port 69) **telnet** (Port 23) **time** (Port 37) **uucp** (Port 540)

	irc (Port 194)	**whois** (Port 43)
	klogin (Port 543)	**www** (Port 80)
	kshell (Port 544)	
	login (Port 513)	

<destination> Specifies the destination used for packet matching. Destinations can be expressed in one of four ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** *<ip address>* to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the *<ip address>* *<wildcard mask>* format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** *<hostname>* to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** *<name>* in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<destination port> Optional. Specifies the destination port. Only valid when *<protocol>* is **tcp** or **udp.** The same keywords and port numbers/names used for the *<source port>* field are valid for the *<destination port>* field. Refer to previously listed *<source port>* for more details.

fragments Optional. Indicates that the IPv4 ACL entry will only be matched by non-initial fragments. This parameter is only available using the **ip** protocol.

log Optional. Enables logging of any packets that match the IPv4 ACL entry.

track *<name>* Optional. Makes the IPv4 ACL entry dependent upon a track.

Default Values

By default, all AOS IPv4 security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.
Release 16.1	Command was expanded to include the **log**, **track**, and **vrf** parameters.
Release R11.10.2	Command was expanded to include the **fragments** parameter.

Functional Notes

IPv4 Access control lists (ACLs) are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv4 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv4 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** IPv4 ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** IPv4 ACL advances AOS to the next access policy entry. AOS provides two types of IPv4 ACLs: standard and extended. Standard IPv4 ACLs match based on the source of the packet. Extended IPv4 ACLs match based on the source and destination of the packet.

IPv4 ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF will only affect the default unnamed VRF.

IPv4 ACLs match non-initial fragments in the following manner:

- Non-initial fragments can match entries with the **fragments** keyword, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments can match entries with the **ip** protocol specified, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments are implicitly permitted by access groups if the fragments did not match an explicit entry in the ACL.

Usage Examples

The following example creates an ACL **DenyIKE** to deny all Internet key exchange (IKE) (UDP Port 500) packets from the 190.72.22.0 /24 network:

(config)**#ip access-list extended DenyIKE**
(config-ext-nacl)**#deny udp 190.72.22.0 0.0.0.255 eq 500 any eq 500**

The following example creates an entry in the **Untrusted** IPv4 ACL to deny ip packets from host name **www.adtran.com** using the nondefault VRF **RED** to resolve the DNS host name with any destination:

(config)**#ip access-list extended Untrusted**
(config-ext-nacl)**#deny ip hostname www.adtran.com vrf RED any**

deny icmp <*source*> <*destination*>

Use the **deny icmp** command to configure the extended Internet Protocol version 4 (IPv4) access control list (ACL) to deny specified Internet Control Message Protocol (ICMP) packets entry into the routing system. This command provides traffic matching based on the packet's IPv4 header field and ICMP-specific fields. Use the **no** form of this command to remove the deny parameter from the IPv4 ACL. Variations of this command include:

deny icmp <*source*> <*destination*>
deny icmp <*source*> <*destination*> <*message name*>
deny icmp <*source*> <*destination*> <*message type*> <*message code*>

Syntax Description

<*source*>

Specifies the source used for IPv4 packet matching. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** <*ipv4 address*> to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the <*ip address*> <*wildcard mask*> format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** <*hostname*> to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** <*name*> in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<*destination*>

Specifies the destination used for packet matching. Destinations can be expressed in one of five ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** <*ip address*> to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the <*ip address*> <*wildcard mask*> format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** <*hostname*> to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** <*name*> in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<message name> Optional. Specifies the ICMP message type used for matching ICMP packets. ICMP message names are specified using one of the following keywords:

administratively-prohibited	Indicates the destination is unreachable because it is administratively prohibited.
alternate-address	Indicates the destination has an alternate address.
conversion-error	Indicates an error in datagram conversion.
dod-host-prohibited	Indicates the host is prohibited.
dod-net-prohibited	Indicates the network is prohibited.
echo	Indicates an echo (ping) message.
echo-reply	Indicates an echo reply message.
host-isolated	Indicates the host is isolated.
host-redirect	Indicates the host is redirected.
host-tos-redirect	Indicates the host is redirected for type of service (TOS).
host-tos-unreachable	Indicates the host is unreachable for TOS.
host-unknown	Indicates the host is unknown.
host-unreachable	Indicates the host is unreachable.
information-reply	Indicates an information reply.
information-request	Indicates an information request.
log	Indicates the log matches against this entry.
mask-reply	Indicates an address mask reply.
mask-request	Indicates an address mask request.
mobile-redirect	Indicates a mobile host redirect.
net-redirect	Indicates a network redirect.
net-tos-redirect	Indicates a network redirect for TOS.
net-tos-unreachable	Indicates the network is unreachable for TOS.
net-unreachable	Indicates the network is unreachable.
network-unknown	Indicates the network is unknown.

option-missing	Indicates a parameter that is required is missing.
packet-too-big	Indicates the packet is too large. Fragmentation is needed and the DF should be set.
port-unreachable	Indicates the destination is unreachable because the port is unreachable.
precedence-unreachable	Indicates the precedence is cut off.
protocol-unreachable	Indicates the protocol is unreachable.
reassembly-timeout	Indicates a timeout for reassembly.
redirect	Indicates a redirect message.
router-advertisement	Indicates a router advertisement message.
router-solicitation	Indicates an router solicitation message.
source-quench	Indicates a source quench.
source-route-failed	Indicates the source route failed.
timestamp-reply	Indicates a timestamp reply.
timestamp-request	Indicates a timestamp request.
traceroute	Indicates a traceroute.
track	Indicates this ACL entry is dependent upon a track.
ttl-exceeded	Indicates the time-to-live (TTL) value has been exceeded.
unreachable	Indicates the destination is unreachable.

<message type>	Optional. Specifies the ICMP message type for matching ICMP packets. When you specify an ICMP message type, you must also specify an ICMP message code. Message types range from **0** to **127** for error messages and from **128** to **255** for informational messages.
<message code>	Optional. Specifies the ICMP message code for matching ICMP packets. You must specify the message code when you specify the ICMP message type. Message code range is **0** to **255**.

Default Values

By default, all AOS IPv4 security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release R11.1.0	Command was introduced.

Functional Notes

IPv4 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv4 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv4 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv4 ACLs: standard and extended. Standard IPv4 ACLs match based on the source of the packet. Extended IPv4 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an extended IPv4 ACL named **Untrustedv4** IPv4 ACL that denies any IPv4 traffic from a source with the address **10.10.10.1**, headed to a destination of **10.10.10.4**, and an ICMP message type of **echo-reply**:

(config)**#ipv4 access-list extended Untrustedv4**
(config-ext6-nacl)**#deny icmp 10.10.10.1 10.10.10.4 echo-reply**

permit *<protocol> <source> <source port> <destination> <destination port>*

Use the **permit** command to configure the extended Internet Protocol version 4 (IPv4) access control list (ACL) to permit specified packets entry into the routing system. Use the **no** form of this command to remove the permit permission from the IPv4 ACL. Variations of this command include:

permit *<protocol> <source> <source port> <destination> <destination port>*
permit *<protocol> <source> <source port> <destination> <destination port>* **log**
permit *<protocol> <source> <source port> <destination> <destination port>* **track** *<name>*
permit ip *<source> <source port> <destination> <destination port>* **fragments**

Syntax Description

<protocol> Specifies the IPv4 data protocol **ip**, **tcp**, **udp**, **ahp**, **esp**, **gre**, or a specific protocol. Range is **0** to **255**.

<source> Specifies the source used for IPv4 packet matching. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** *<ip address>* to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the *<ip address> <wildcard mask>* format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** *<hostname>* to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** *<name>* in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<source port> Optional. The source port is used only when *<protocol>* is **tcp** or **udp**. The following keywords and port numbers/names are supported for the *<source port>* field:

any	Matches any destination port.
eq *<port number/name>*	Matches only packets equal to specified port number.
gt *<port number/name>*	Matches only packets with a port number greater than the specified port number.
lt *<port number/name>*	Matches only packets with a port number less than the specified port number.
neq *<port number/name>*	Matches only packets that are not equal to the specified port number.
range *<begin port number/name> <endport number/name>*	Matches only packets that contain a port number in the specified range.

<port number>	Specifies the port number used by Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) to pass information to upper layers using the following syntax: <***0-65535***>. All ports below 1024 are considered well-known ports, and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above 1024 are dynamically assigned ports that include registered ports for vendor-specific applications.
<port name>	The following UDP port numbers can be specified using the associated names: **biff** (Port 512) **bootpc** (Port 68) **bootps** (Port 67) **discard** (Port 9) **dnsix** (Port 195) **domain** (Port 53) **echo** (Port 7) **isakmp** (Port 500) **mobile-ip** (Port 434) **nameserver** (Port 42) **netbios-dgm** (Port 138) **netbios-ns** (Port 137) **netbios-ss** (Port 139) **ntp** (Port 123) **pim-auto-rp** (Port 496) **rip** (Port 520) **snmp** (Port 161) **snmptrap** (Port 162) **sunrpc** (Port 111) **syslog** (Port 514) **tacacs** (Port 49) **talk** (Port 517) **tftp** (Port 69) **time** (Port 37) **who** (Port 513) **xdmcp** (Port 177) The following TCP port numbers can be specified using the associated names: **bgp** (Port 179) **chargen** (Port 19) **cmd** (Port 514) **daytime** (Port 13) **discard** (Port 9) **domain** (Port 53) **echo** (Port 7) **exec** (Port 512) **finger** (Port 79) **ftp** (Port 21) **gopher** (Port 70) **hostname** (Port 101) **ident** (Port 113) **lpd** (Port 515) **nntp** (Port 119) **pim-auto-rp** (Port 496) **pop2** (Port 109) **pop3** (Port 110) **smtp** (Port 25) **sunrpc** (Port 111) **tacacs** (Port 49) **talk** (Port 517) **tftp** (Port 69) **telnet** (Port 23) **time** (Port 37) **uucp** (Port 540)

		irc (Port 194)	**whois** (Port 43)
		klogin (Port 543)	**www** (Port 80)
		kshell (Port 544)	
		login (Port 513)	

<destination> Specifies the destination used for IPv4 packet matching. Destinations can be expressed in one of five ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** *<ip address>* to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the *<ip address>* *<wildcard mask>* format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** *<hostname>* to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** *<name>* in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<destination port> Optional. Specifies the destination port. Only valid when *<protocol>* is **tcp** or **udp.** The same keywords and port numbers/names used for the *<source port>* field are valid for the *<destination port>* field. Refer to previously listed *<source port>* for more details.

fragments Optional. Indicates that the IPv4 ACL entry will only be matched by non-initial fragments. This parameter is only available using the **ip** protocol.

log Optional. Enables logging of any packets that match the IPv4 ACL entry.

track *<name>* Optional. Makes the IPv4 ACL entry dependent upon a track.

Default Values

By default, all AOS security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.
Release 16.1	Command was expanded to include the **log**, **track**, and **vrf** parameters.
Release R11.10.2	Command was expanded to include the **fragments** parameter.

Functional Notes

IPv4 Access control lists (ACLs) are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv4 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv4 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** IPv4 ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** IPv4 ACL advances AOS to the next access policy entry. AOS provides two types of IPv4 ACLs: standard and extended. Standard IPv4 ACLs match based on the source of the packet. Extended IPv4 ACLs match based on the source and destination of the packet.

IPv4 ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF will only affect the default unnamed VRF.

IPv4 ACLs match non-initial fragments in the following manner:

- Non-initial fragments can match entries with the **fragments** keyword, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments can match entries with the **ip** protocol specified, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments are implicitly permitted by access groups if the fragments did not match an explicit entry in the ACL.

Usage Examples

The following example creates an IPv4 ACL **AllowIKE** to allow all Internet key exchange (IKE) (UDP Port 500) packets from the 190.72.22.0 /24 network:

(config)**#ip access-list extended AllowIKE**
(config-ext-nacl)**#permit udp 190.72.22.0 0.0.0.255 eq 500 any eq 500**

The following example creates an entry in the **MatchAll** IPv4 ACL to permit ip packets from host name **www.adtran.com** using the nondefault VRF **RED** to resolve the DNS host name with any destination:

(config)**#ip access-list extended MatchAll**
(config-ext-nacl)**#permit ip hostname www.adtran.com vrf RED any**

permit icmp <*source*> <*destination*>

Use the **permit icmp** command to configure the extended Internet Protocol version 4 (IPv4) access control list (ACL) to permit specified Internet Control Message Protocol (ICMP) packets entry into the routing system. This command provides traffic matching based on the packet's IPv4 header field and ICMP-specific fields. Use the **no** form of this command to remove the permit parameter from the IPv4 ACL. Variations of this command include:

permit icmp <*source*> <*destination*>
permit icmp <*source*> <*destination*> <*message name*>
permit icmp <*source*> <*destination*> <*message type*> <*message code*>

Syntax Description

<*source*>

Specifies the source used for IPv4 packet matching. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** <*ipv4 address*> to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the <*ip address*> <*wildcard mask*> format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** <*hostname*> to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** <*name*> in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<*destination*>

Specifies the destination used for packet matching. Destinations can be expressed in one of five ways:

1. Using the keyword **any** to match any IPv4 address.
2. Using **host** <*ip address*> to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
3. Using the <*ip address*> <*wildcard mask*> format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**).
4. Using the keyword **hostname** <*hostname*> to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** <*name*> in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.

<message name> Optional. Specifies the ICMP message type used for matching ICMP packets. ICMP message names are specified using one of the following keywords:

administratively-prohibited	Indicates the destination is unreachable because it is administratively prohibited.
alternate-address	Indicates the destination has an alternate address.
conversion-error	Indicates an error in datagram conversion.
dod-host-prohibited	Indicates the host is prohibited.
dod-net-prohibited	Indicates the network is prohibited.
echo	Indicates an echo (ping) message.
echo-reply	Indicates an echo reply message.
host-isolated	Indicates the host is isolated.
host-redirect	Indicates the host is redirected.
host-tos-redirect	Indicates the host is redirected for type of service (TOS).
host-tos-unreachable	Indicates the host is unreachable for TOS.
host-unknown	Indicates the host is unknown.
host-unreachable	Indicates the host is unreachable.
information-reply	Indicates an information reply.
information-request	Indicates an information request.
log	Indicates the log matches against this entry.
mask-reply	Indicates an address mask reply.
mask-request	Indicates an address mask request.
mobile-redirect	Indicates a mobile host redirect.
net-redirect	Indicates a network redirect.
net-tos-redirect	Indicates a network redirect for TOS.
net-tos-unreachable	Indicates the network is unreachable for TOS.
net-unreachable	Indicates the network is unreachable.
network-unknown	Indicates the network is unknown.

option-missing	Indicates a parameter that is required is missing.
packet-too-big	Indicates the packet is too large. Fragmentation is needed and the DF should be set.
port-unreachable	Indicates the destination is unreachable because the port is unreachable.
precedence-unreachable	Indicates the precedence is cut off.
protocol-unreachable	Indicates the protocol is unreachable.
reassembly-timeout	Indicates a timeout for reassembly.
redirect	Indicates a redirect message.
router-advertisement	Indicates a router advertisement message.
router-solicitation	Indicates an router solicitation message.
source-quench	Indicates a source quench.
source-route-failed	Indicates the source route failed.
timestamp-reply	Indicates a timestamp reply.
timestamp-request	Indicates a timestamp request.
traceroute	Indicates a traceroute.
track	Indicates this ACL entry is dependent upon a track.
ttl-exceeded	Indicates the time-to-live (TTL) value has been exceeded.
unreachable	Indicates the destination is unreachable.

<message type>	Optional. Specifies the ICMP message type for matching ICMP packets. When you specify an ICMP message type, you must also specify an ICMP message code. Message types range from **0** to **127** for error messages and from **128** to **255** for informational messages.
<message code>	Optional. Specifies the ICMP message code for matching ICMP packets. You must specify the message code when you specify the ICMP message type. Message code range is **0** to **255**.

Default Values

By default, all AOS IPv4 security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release R11.1.0	Command was introduced.

Functional Notes

IPv4 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv4 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv4 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv4 ACLs: standard and extended. Standard IPv4 ACLs match based on the source of the packet. Extended IPv4 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an extended IPv4 ACL named **Untrustedv4** IPv4 ACL that permits any IPv4 traffic from a source with the address **10.10.10.1**, headed to a destination of **10.10.10.4**, and an ICMP message type of **echo-reply**:

(config)**#ipv4 access-list extended Untrustedv4**
(config-ext6-nacl)**#permit icmp 10.10.10.1 10.10.10.4 echo-reply**

remark *<remark>*

Use the **remark** command to associate a descriptive tag with an extended Internet Protocol version 4 (IPv4) access control list (ACL). Use the **no** form of this command to remove the descriptive tag.

Syntax Description

<remark>	Specifies a descriptive tag for the IPv4 ACL. Tags can be up to **80** alphanumeric characters enclosed in quotation marks. For example, “This list blocks all outbound Web traffic.”

Default Values

By default, all AOS security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a description for extended IPv4 ACL **matchall**:

(config)**#ip access-list extended matchall**
(config-ext-nacl)**#remark “allows all ip traffic from remote location”**

deny *<source>*

Use the **deny** command to configure the standard Internet Protocol version 4 (IPv4) access control list (ACL) to deny specified packets entry into the routing system. Use the **no** form of this command to remove the deny parameter from the IPv4 ACL. Variations of this command include:

deny <*source*>
deny <*source*> **log**
deny <*source*> **track** <*name*>

Syntax Description

<*source*>	Specifies the source used for IPv4 packet matching. Sources can be expressed in one of four ways: 1. Using the keyword **any** to match any IPv4 address. 2. Using **host** <*ip address*> to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). 3. Using the <*ip address*> <*wildcard mask*> format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**). 4. Using the keyword **hostname** <*hostname*> to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** <*name*> in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.
log	Optional. Enables logging of any packets that match the IPv4 ACL entry.
track <*name*>	Optional. Makes the IPv4 ACL entry dependent upon a track.

Default Values

By default, all AOS security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.
Release 16.1	Command was expanded to include the **log**, **track**, and **vrf** parameters.

Functional Notes

IPv4 Access control lists (ACLs) are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv4 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv4 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** IPv4 ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** IPv4 ACL advances AOS to the next access policy entry. AOS provides two types of IPv4 ACLs: standard and extended. Standard IPv4 ACLs match based on the source of the packet. Extended IPv4 ACLs match based on the source and destination of the packet.

IPv4 ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example creates an IPv4 ACL **UnTrusted** to deny all packets from the 190.72.22.248 /30 network:

(config)**#ip access-list standard UnTrusted**
(config-std-nacl)**#deny 190.72.22.248 0.0.0.3**

permit <*source*>

Use the **permit** command to configure the standard Internet Protocol version 4 (IPv4) access control list (ACL) to permit specified packets entry into the routing system. Use the **no** form of this command to remove the permit permission from the IPv4 ACL. Variations of this command include:

permit <*source*>
permit <*source*> **log**
permit <*source*> **track** <*name*>

Syntax Description

<*source*>	Specifies the source used for IPv4 packet matching. Sources can be expressed in one of four ways: 1. Using the keyword **any** to match any IPv4 address. 2. Using **host** <*ip address*> to specify a single host address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). 3. Using the <*ip address*> <*wildcard mask*> format to match all IPv4 addresses in a range. The wildcard mask corresponds to a range of IPv4 addresses (network) or a specific host. Wildcard masks are expressed in dotted decimal notation (for example, **0.0.0.255**). 4. Using the keyword **hostname** <*hostname*> to match based on a DNS name. The unit must be configured with DNS servers for this function to work. Using **vrf** <*name*> in conjunction with the **hostname** parameter associates a nondefault VRF with the DNS host name for the source. The VRF is required if the router's DNS server is on a nondefault VRF. This parameter can only be used with the **hostname** source.
log	Optional. Enables logging of any packets that match the IPv4 ACL entry.
track <*name*>	Optional. Makes the IPv4 ACL entry dependent upon a track.

Default Values

By default, all AOS security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.
Release 16.1	Command was expanded to include the **log**, **track**, and **vrf** parameters.

Functional Notes

IPv4 Access control lists (ACLs) are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv4 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv4 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** IPv4 ACL is used to match packets (meeting the specified pattern) to enter the router system. A **deny** IPv4 ACL advances AOS to the next access policy entry. AOS provides two types of IPv4 ACLs: standard and extended. Standard IPv4 ACLs match based on the source of the packet. Extended IPv4 ACLs match based on the source and destination of the packet.

IPv4 ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF will only affect the default unnamed VRF.

Usage Examples

The following example creates an IPv4 ACL **Trusted** to permit all packets from the 190.72.22.248 /30 network:

(config)**#ip access-list standard Trusted**
(config-std-nacl)**#permit 190.72.22.248 0.0.0.3**

remark *<remark>*

Use the **remark** command to associate a descriptive tag with a standard Internet Protocol version 4 (IPv4) access control list (ACL). Use the **no** form of this command to remove the descriptive tag.

Syntax Description

<remark>	Specifies a descriptive tag for the IPv4 ACL. Tags can be up to **80** alphanumeric characters enclosed in quotation marks. For example, “This list blocks all outbound Web traffic.”

Default Values

By default, all AOS security features are disabled, and there are no configured IPv4 ACLs.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a description for standard IPv4 ACL **matchall**:

(config)**#ip access-list extended matchall**
(config-std-nacl)**#remark “allows all ip traffic from remote location”**

IPv4 Access Control Policy Command Set

An Internet Protocol version 4 (IPv4) access control policy (ACP) defines a policy class containing IPv4 access control lists (ACLs) in the Adtran Operating System (AOS) command line interface (CLI). The IPv4 ACP is a named policy with multiple action entries.

IPv6 ACPs are also supported by AOS, but are explained separately in this document. Refer to *IPv6 Access Control Policy Command Set on page 4326* for more information on configuring IPv6 ACPs.

To create an IPv4 ACP and activate the Access Control Policy Configuration mode, enter the **ip policy-class** <*ipv4 acp name*> command at the Global Configuration mode prompt. For example:

```
>enable
#config terminal
(config)#ip policy-class PRIVATE
(config-policy-class)#
```

> NOTE
> *Configured IPv4 ACPs will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

> CAUTION
> *Before applying an IPv4 ACP to an interface, verify your Telnet or secure shell (SSH) connection will not be affected by the policy. If an IPv4 ACP is applied to the interface you are connecting through and it does not allow Telnet or SSH traffic, your connection will be lost.*

Technology Review

IPv4 ACPs and IPv4 ACLs regulate traffic through the routed network. When designing your traffic flow configuration, it is important to keep the following in mind:

- An IPv4 ACL serves as a packet selector, defining exactly which packets should take the given action.
- An IPv4 ACP defines the action to take on the packets selected by the IPv4 ACL.
- An IPv4 ACL is inactive until it is assigned to an active IPv4 ACP.
- An IPv4 ACP is inactive until it is assigned to an interface.

IPv4 Access Control Policies (ACPs)

IPv4 ACPs are used to allow, discard, or manipulate (using network address translation (NAT)) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (IPv4 ACL). In a sense, the IPv4 ACPs answer the question, “What should I do?” while the IPv4 ACLs answer the question, “On which packets?”

When packets are received on an interface with an IPv4 ACP applied, the IPv4 ACP is used to determine whether the data is processed or discarded. Both IPv4 ACLs and IPv4 ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed. The IPv4 ACP has an implicit **discard** at the end of the list. Typically, the most specific entries should be at the top and the most general at the bottom.

IPv4 Access Control Lists (ACLs)

IPv4 ACLs are used as packet selectors by IPv4 ACPs. They must be assigned to an IPv4 ACP in order to be active.

IPv4 ACP must use an IPv4 ACL. You cannot apply an IPv4 ACL to an IPv6 ACP, or vice-versa. In addition, all IPv4 ACLs and IPv4 ACPs must have a different name than any configured IPv6 ACLs or IPv6 ACPs.

IPv4 ACLs are composed of an ordered list of entries. Each entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** action is used to allow packets (meeting the specified pattern) to enter the router system. A **deny** action is used to disregard packets (that do not match the pattern) and proceed to the next entry on the IPv4 ACP. The IPv4 ACL has an implicit **deny** at the end of the list.

The AOS provides two types of IPv4 ACLs: **standard** and **extended**. A **standard** IPv4 ACL allows source IPv4 address packet patterns only. An **extended** IPv4 ACL may specify patterns using most fields in the IPv4 header and the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) header.

Creating and Assigning IPv4 ACLs and IPv4 ACPs

Creating IPv4 ACPs and IPv4 ACLs to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of AOS using the **ip firewall** command. Refer to the command *ip firewall on page 1367* for more information.

Step 2:
Create an IPv4 ACP that uses a configured IPv4 ACL by issuing the **ip policy-class** command. AOS IPv4 ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (IPv4 ACL). When packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

Step 3:
Create an IPv4 ACL to permit or deny specified traffic by using either the **ip access-list extended** or **ip access-list standard** command. Standard IPv4 ACLs match based on the source IPv4 address of the packet. Extended IPv4 ACLs match based on the source and destination of the packet. Refer to the command *ip access-list extended <ipv4 acl name> on page 1344* or the command *ip access-list standard <ipv4 acl name> on page 1346* for more information. Sources can be expressed in one of four ways:

1. Using the keyword **any** to match any IPv4 address.

2. Using **host** <*ipv4 address*> to specify a single host address.

3. Using the <*ipv4 address*> <*wildcard*> format to match all IPv4 addresses in a range. Wildcard masks work in reverse logic from subnet masks. When broken out into binary form, a 0 indicates which bits of the IPv4 address to consider, a 1 indicates which bits are disregarded. For example, specifying 255 in any octet of the wildcard mask equates to a “don’t care” for that octet in the IPv4 address. Additionally, a 30-bit mask would be represented with the wildcard string 0.0.0.3, a 28-bit mask with 0.0.0.15, a 24-bit mask with 0.0.0.255, and so forth.

4. Using the keyword **hostname** to match based on a domain naming system (DNS) name. DNS servers must be configured or host names must be locally defined for this function to work.

Step 4:
Apply the created IPv4 ACP to an interface. To assign an IPv4 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ip access-policy** <*ipv4 acp name*>. The following example assigns ACP **UNTRUSTED** to the Ethernet 0/1 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip access-policy UNTRUSTED**

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

allow list on page 4281
allow reverse list on page 4283
discard list on page 4285
nat destination list on page 4287
nat destination list <ipv4 acl name> pool <pool name> on page 4289
nat source list on page 4291
nat source list <ipv4 acl name> pool <pool name> on page 4294

allow list

Use the **allow list** command to specify an Internet Protocol version 4 (IPv4) access control list (ACL) to determine which packets are allowed to enter the interface to which the IPv4 access control policy (ACP) is assigned, and create a firewall association in the firewall. All associations created by the **allow list** command are subject to the built-in firewall timers (refer to *ip policy-timeout on page 1439*). Variations of this command include:

allow list *<ipv4 acl name>*
allow list *<ipv4 acl name>* **policy** *<ipv4 acp name>*
allow list *<ipv4 acl name>* **policy** *<ipv4 acp name>* **stateless**
allow list *<ipv4 acl name>* **self**
allow list *<ipv4 acl name>* **self stateless**
allow list *<ipv4 acl name>* **stateless**

Syntax Description

<ipv4 acl name>	Specifies the IPv4 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
policy *<ipv4 acp name>*	Optional. Specifies the destination IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the packet's egress interface as determined by the routing table or policy-based routing configuration. If there is a match, the firewall will process the packet. If there is no match, the firewall will process the packet based on the next IPv4 ACP entry or implicitly discard it if no further IPv4 ACP entries exist.
self	Optional. Allows packets to pass that are permitted by the IPv4 ACL and destined for any local interface on the unit. These packets are terminated by the unit and are not routed or forwarded to other destinations. Using the **self** keyword is helpful when opening up remote administrative access to the unit (Telnet, secure shell (SSH), Internet Control Message Protocol (ICMP), Web-based graphical user interface (GUI)).
stateless	Optional. Enables bypassing of stateful firewall processing and application-level gateways (ALGs). Use for trusted traffic or traffic that the firewall is incorrectly blocking as a perceived attack. Stateless processing is helpful when passing traffic over virtual private network (VPN) tunnels. Traffic sent over VPN tunnels is purposely selected and encrypted; there is no need for additional inspection of the traffic by the firewall. VPN configurations created using the VPN Wizard in the GUI use stateless processing by default.

Default Values

By default, all AOS security features are disabled and there are no configured IPv4 ACP entries.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example configures the IPv4 ACP name **UNTRUSTED** to allow any traffic that matches the IPv4 ACL named **INWEB** to enter the router system:

(config)**#ip policy-class UNTRUSTED**
(config-policy-class)**#allow list INWEB**

allow reverse list

Use the **allow reverse list** command to specify an Internet Protocol version 4 (IPv4) access control list (ACL) to determine which packets are allowed to enter the interface to which the IPv4 access control policy (ACP) is assigned, and create a firewall association in the firewall. The **allow reverse list** command is identical in function to the **allow list** command with the exception of the **reverse** keyword. The **reverse** keyword instructs the firewall to use the source information as the destination information and vice versa when attempting matches against the specified IPv4 ACL. This command is most useful when the IPv4 ACP is applied to an interface terminating a virtual private network (VPN) tunnel. The **allow reverse list** allows the reuse of the IPv4 ACL defined as the VPN selector. Variations of this command include:

allow reverse list *<ipv4 acl name>*
allow reverse list *<ipv4 acl name>* **policy** *<ipv4 acp name>*
allow reverse list *<ipv4 acl name>* **policy** *<ipv4 acp name>* **stateless**
allow reverse list *<ipv4 acl name>* **self**
allow reverse list *<ipv4 acl name>* **self stateless**
allow reverse list *<ipv4 acl name>* **stateless**

Syntax Description

<ipv4 acl name>	Specifies the IPv4 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
policy *<ipv4 acp name>*	Optional. Specifies the destination IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the packet's egress interface as determined by the routing table or policy-based routing configuration. If there is a match, the firewall will process the packet. If there is no match, the firewall will process the packet based on the next IPv4 ACP entry or implicitly discard it if no further IPv4 ACP entries exist.
self	Optional. Allows packets to pass that are permitted by the IPv4 ACL and destined for any local interface on the unit. These packets are terminated by the unit and are not routed or forwarded to other destinations. Using the **self** keyword is helpful when opening up remote administrative access to the unit (Telnet, secure shell (SSH), Internet Control Message Protocol (ICMP), Web-based graphical user interface (GUI)).
stateless	Optional. Enables bypassing of stateful firewall processing and application-level gateways (ALGs). Use for trusted traffic or traffic that the firewall is incorrectly blocking as a perceived attack. Stateless processing is helpful when passing traffic over VPN tunnels. Traffic sent over VPN tunnels is purposely selected and encrypted; there is no need for additional inspection of the traffic by the firewall. VPN configurations created using the VPN Wizard in the GUI use stateless processing by default.

Default Values

By default, all AOS security features are disabled and there are no configured IPv4 ACP entries.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example configures the IPv4 ACP named **UNTRUSTED** to allow any traffic that matches the IPv4 ACL named **INWEB** (with source and destination information reversed) to enter the router system:

(config)**#ip policy-class UNTRUSTED**
(config-policy-class)**#allow reverse list INWEB**

discard list

Use the **discard list** command to specify an Internet Protocol version 4 (IPv4) access control list (ACL) to determine which packets are discarded after entering the interface to which the IPv4 access control policy (ACP) is assigned. Packets matched by the IPv4 ACL will be discarded, and no further IPv4 ACP entries will be inspected. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist. Variations of this command include:

discard list <*ipv4 acl name*>
discard list <*ipv4 acl name*> **policy** <*ipv4 acp name*>
discard list <*ipv4 acl name*> **self**

Syntax Description

<*ipv4 acl name*>	Specifies the IPv4 ACL against which to check traffic before discarding the packet. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
policy <*ipv4 acp name*>	Optional. Specifies the destination IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the packet's egress interface as determined by the routing table or policy-based routing configuration. If there is a match, the firewall will discard the packet. If there is no match, the firewall will process the packet based on the next IPv4 ACP entry or implicitly discard it if no further IPv4 ACP entries exist.
self	Optional. Discards packets that are matched by the IPv4 ACL and destined for any local interface on the unit. These packets, had they been allowed, would be terminated by the unit and not routed or forwarded to other destinations. Using the **self** keyword is helpful when forbidding certain access to the unit.

Default Values

By default, all AOS security features are disabled and there are no configured IPv4 ACP entries.

Command History

Release 2.1	Command was introduced.

Functional Notes

AOS IPv4 ACPs are used to allow, discard, or manipulate (using network address translation (NAT)) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (IPv4 ACL). When packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

*An implicit discard exists at the end of every IPv4 ACP. Specifying a **discard list** is unnecessary in most applications and should be used with caution. A **discard list** can adversely affect certain functions of a unit (virtual private network (VPN), routing protocols, etc.). Specifying an empty IPv4 ACL or a nonexistent IPv4 ACL in an IPv4 ACP will result in an implicit permit.*

Usage Examples

The following example configures the IPv4 ACP named **UNTRUSTED** to discard any traffic that matches the IPv4 ACL named **INWEB**:

(config)**#ip policy-class UNTRUSTED**
(config-policy-class)**#discard list INWEB**

nat destination list

Use the **nat destination list** command to translate the destination Internet Protocol version 4 (IPv4) address to a specified IPv4 address, and creates a firewall association in the firewall. The translation is applied only to those packets permitted by the specified IPv4 access control list (ACL) and entering the interface to which the IPv4 access control policy (ACP) is assigned. All firewall associations are subject to the built-in firewall timers (refer to *ip policy-timeout on page 1439*). Variations of this command include:

nat destination list <*ipv4 acl name*> **address** <*ipv4 address*> **no-alg**
nat destination list <*ipv4 acl name*> **address** <*ipv4 address*> **port** <*port number*>
nat destination list <*ipv4 acl name*> **address** <*ipv4 address*> **port** <*port number*> **no-alg**
nat destination list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*>
nat destination list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*> **no-alg**
nat destination list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*> **port** <*port number*>
nat destination list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*> **port** <*port number*> **no-alg**

Syntax Description

<*ipv4 acl name*>	Specifies the IPv4 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
address <*ipv4 address*>	Specifies the address of the private IPv4 host to which the translated packets are destined. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
address vrf <*ipv4 address*> <*vrf name*>	Specifies the virtual routing and forwarding (VRF) instance corresponding to the specified post-NAT destination address.
no-alg	Optional. Allows packets matching the IPv4 ACP entry to traverse the firewall without being processed by the application-level gateways (ALGs). This parameter, along with the appropriate IPv4 ACL, prevents specific destinations from being processed by the ALGs.
port <*port number*>	Optional. Translates the original destination port to a user-specified port.

Default Values

By default, all AOS security features are disabled and there are no configured IPv4 ACP entries.

Command History

Release 2.1	Command was introduced.
Release 16.1	Command was expanded to include the **no-alg** parameter.
Release 17.1	Command was expanded to include the **vrf** parameter.
Release A4.01	Syntax for the **address vrf** parameter was altered.

Functional Notes

AOS IPv4 ACPs are used to allow, discard, or manipulate (using network address translation (NAT)) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (ACL). When packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

*An implicit discard exists at the end of every IPv4 ACP. Specifying a **discard list** is unnecessary in most applications and should be used with caution. A **discard list** can adversely affect certain functions of a unit (VPN, routing protocols, etc.). Specifying an empty IPv4 ACL or a nonexistent IPv4 ACL in an IPv4 ACP will result in an implicit permit.*

The optional **vrf** <*vrf name*> parameter specifies the VRF instance. The VRF does not have to be the same VRF from which the packet originated. VRF on an AOS product allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF indicates that the specified address corresponds to the default unnamed VRF.

Usage Examples

The following example enables NAT for traffic that matches the IPv4 ACL **INWEB** and changes the destination address to **192.168.0.253**:

(config)**#ip policy-class UNTRUSTED**
(config-policy-class)**#nat destination list INWEB address 192.168.0.253**

nat destination list *<ipv4 acl name>* pool *<pool name>*

Use the **nat destination list pool** command to translate the destination Internet Protocol version 4 (IPv4) address to an address within the specified pool of addresses, translating a global to local address association. The translation is applied only to those packets permitted by the specified IPv4 access control list (ACL), and entering the interface to which the IPv4 access control policy (ACP) is assigned, and to those packets whose destination IPv4 address falls within the global range of the network address translation (NAT) pool. All firewall associations are subject to the built-in firewall timers (refer to *ip policy-timeout on page 1439*). Variations of this command include:

nat destination list *<ipv4 acl name>* **pool** *<pool name>*
nat destination list *<ipv4 acl name>* **pool** *<pool name>* **no-alg**

Syntax Description

<ipv4 acl name>	Specifies the IPv4 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
pool *<pool name>*	Specifies the NAT pool to use for address mapping. If the destination IPv4 address does not fall within the global range of the specified pool, the packet will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
no-alg	Optional. Allows packets matching the IPv4 ACP entry to traverse the firewall without being processed by the application-level gateways (ALGs). This parameter, along with the appropriate IPv4 ACL, prevents specific destinations from being processed by the ALGs.

Default Values

By default, all AOS security features are disabled and there are no configured IPv4 ACP entries.

Command History

Release 17.4	Command was introduced.

Functional Notes

AOS IPv4 ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (ACL). When packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

*An implicit discard exists at the end of every IPv4 ACP. Specifying a **discard list** is unnecessary in most applications and should be used with caution. A **discard list** can adversely affect certain functions of a unit (virtual private network (VPN), routing protocols, etc.). Specifying an empty IPv4 ACL or a nonexistent IPv4 ACL in an IPv4 ACP will result in an implicit permit.*

Usage Examples

The following example enables NAT for traffic that matches the IPv4 ACL **OUTSIDE** and uses the NAT pool **POOL1** to map addresses:

(config)**#ip policy-class PUBLIC**
(config-policy-class)**#nat destination list OUTSIDE pool POOL1**

nat source list

Use the **nat source list** command to translate the source Internet Protocol version 4 (IPv4) address to a specified IPv4 address (or to the primary IPv4 address of the specified interface) and create an association in the firewall. The translation is applied only to those packets permitted by the specified IPv4 access control list (ACL), and entering the interface to which the IPv4 access control policy (ACP) is assigned. This function is commonly referred to as a "many-to-one NAT". All firewall associations are subject to the built-in firewall timers (refer to *ip policy-timeout on page 1439*). Variations of this command include:

nat source list <*ipv4 acl name*> **address** <*ipv4 address*> **overload**
nat source list <*ipv4 acl name*> **address** <*ipv4 address*> **overload no-alg**
nat source list <*ipv4 acl name*> **address** <*ipv4 address*> **overload no-alg policy** <*ipv4 acp name*>
nat source list <*ipv4 acl name*> **address** <*ipv4 address*> **overload policy** <*ipv4 acp name*>
nat source list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*> **overload**
nat source list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*> **overload no-alg**
nat source list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*> **overload no-alg policy** <*ipv4 acp name*>
nat source list <*ipv4 acl name*> **address vrf** <*ipv4 address*> <*vrf name*> **overload policy** <*ipv4 acp name*>
nat source list <*ipv4 acl name*> **interface** <*interface*> **overload**
nat source list <*ipv4 acl name*> **interface** <*interface*> **overload no-alg**
nat source list <*ipv4 acl name*> **interface** <*interface*> **overload no-alg policy** <*ipv4 acp name*>
nat source list <*ipv4 acl name*> **interface** <*interface*> **overload policy** <*ipv4 acp name*>

Syntax Description

<*ipv4 acl name*>	Specifies the IPv4 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
address <*ipv4 address*>	Specifies the IPv4 address from which the translated packets will be sourced. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
address vrf <*ipv4 address*> <*vrf name*>	Specifies the virtual routing and forwarding (VRF) instance corresponding to the specified post-NAT source address.
interface <*interface*>	Specifies the interface from which the translated packets will be sourced. The primary IPv4 address of an interface is used as the source IPv4 address for translated packets. Specify an interface in the format <*interface type* [*slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id*]>. For example, for an Ethernet subinterface, use **eth 0/1.1**; for a PPP interface, use **ppp 1**; and for an ATM subinterface, use **atm 1.1**. Type **nat source list** <*ipv4 acl name*> **interface ?** for a list of valid interfaces.

policy *<ipv4 acp name>*	Optional. Specifies the IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the packet's egress interface as determined by the routing table or policy-based routing configuration. If there is a match, the firewall will process the packet. If there is no match, the firewall will process the packet based on the next IPv4 ACP entry or implicitly discard it if no further IPv4 ACP entries exist.
overload	Allows multiple source IPv4 addresses to be replaced with the single IPv4 address specified or the primary IPv4 address of the specified interface. This conceals private IPv4 addresses from acl nameoutside the local network. The **overload** command is not optional and must be used when using the **nat source list** command with a single address or interface. To perform static 1:1 NAT, use a network address translation (NAT) pool instead (refer to *nat source list <ipv4 acl name> pool <pool name> on page 4294*).
no-alg	Optional. Allows packets matching the IPv4 ACP entry to traverse the firewall without being processed by the application-level gateways (ALGs). This parameter, along with the appropriate IPv4 ACL, prevents specific sources from being processed by the ALGs. For example, this option can be used to prevent specific hosts from being uniform resource locator (URL) filtered by configuring an IPv4 ACP entry with the **no-alg** parameter that matches specific hosts followed by another IPv4 ACP entry that matches remaining hosts. The **no-alg** parameter can be placed before or after the **policy** *<acp name>* parameter.

Default Values

By default, all AOS security features are disabled and there are no configured IPv4 ACP entries.

Command History

Release 2.1	Command was introduced.
Release 16.1	Command was expanded to include the **no-alg** parameter.
Release 17.1	Command was expanded to include the **vrf** parameter.
Release A4.01	Command was expanded to include the Metro Ethernet Forum (MEF) Metro Ethernet interface and alter the syntax for the **address vrf** parameter.
Release A5.01	Command was expanded to include the Gigabit Ethernet interface.

Functional Notes

AOS IPv4 ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (ACL). When packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

*An implicit discard exists at the end of every IPv4 ACP. Specifying a **discard list** is unnecessary in most applications and should be used with caution. A **discard list** can adversely affect certain functions of a unit (VPN, routing protocols, etc.). Specifying an empty IPv4 ACL or a nonexistent IPv4 ACL in an IPv4 ACP will result in an implicit permit.*

The optional **vrf** <*vrf name*> parameter specifies the VRF instance corresponding to the specified address. (If an interface is specified, the VRF of that interface is used.) The VRF does not have to be the same VRF from which the packet originated. VRF on an AOS product allows a single physical router to be partitioned into multiple virtual routers. Each router VRF instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF indicates that the specified address corresponds to the default unnamed VRF.

Usage Examples

The following configuration enables NAT for traffic that matches the IPv4 ACL **MATCHALL** and changes the source address to **63.12.1.2**:

(config)**#ip policy-class UNTRUSTED**
(config-policy-class)**#nat source list MATCHALL address 63.12.1.2 overload**

nat source list *<ipv4 acl name>* pool *<pool name>*

Use the **nat source list pool** command to translate the source Internet Protocol version 4 (IPv4) address to an IPv4 address within the specified pool of addresses, translating a local private address to global public address. The translation is applied only to those packets permitted by the specified IPv4 access control list (ACL), and entering the interface to which the IPv4 access control policy (ACP) is assigned and whose source IPv4 address falls within the local range of addresses in the specified pool. All firewall associations are subject to the built-in firewall timers (refer to *ip policy-timeout on page 1439*). Variations of this command include:

nat source list *<ipv4 acl name>* **pool** *<pool name>*
nat source list *<ipv4 acl name>* **pool** *<pool name>* **no-alg**
nat source list *<ipv4 acl name>* **pool** *<pool name>* **no-alg policy** *<ipv4 acp name>*
nat source list *<ipv4 acl name>* **pool** *<pool name>* **policy** *<ipv4 acp name>*
nat source list *<ipv4 acl name>* **pool** *<pool name>* **policy** *<ipv4 acp name>* **no-alg**

Syntax Description

<ipv4 acl name>	Specifies the IPv4 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the IPv4 ACL will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
pool *<pool name>*	Specifies the network address translation (NAT) pool to use for address mapping. If the source IPv4 address does not fall within the local range of the specified pool, the packet will be processed by the next IPv4 ACP entry or implicitly discarded if no further IPv4 ACP entries exist.
policy *<ipv4 acp name>*	Optional. Specifies the IPv4 ACP against which to match traffic. The firewall attempts to match the specified IPv4 ACP with the IPv4 ACP that is applied to the packet's egress interface as determined by the routing table or policy-based routing configuration. If there is a match, the firewall will process the packet. If there is no match, the firewall will process the packet based on the next IPv4 ACP entry or implicitly discard it if no further IPv4 ACP entries exist.
no-alg	Optional. Allows packets matching the IPv4 ACP entry to traverse the firewall without being processed by the application-level gateways (ALGs). This parameter, along with the appropriate IPv4 ACL, prevents specific sources from being processed by the ALGs. For example, this option can be used to prevent specific hosts from being uniform resource locator (URL) filtered by configuring an IPv4 ACP entry with the **no-alg** parameter that matches specific hosts followed by another IPv4 ACP entry that matches remaining hosts. The **no-alg** parameter can be placed before or after the **policy** *<acp name>* parameter.

Default Values

By default, all AOS security features are disabled and there are no configured IPv4 ACP entries.

Command History

Release 17.4	Command was introduced.

Functional Notes

AOS IPv4 ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each IPv4 ACP consists of an action (**allow**, **discard**, **nat**) and a selector (ACL). When packets are received on an interface, the configured IPv4 ACPs are applied to determine whether the data will be processed or discarded.

*An implicit discard exists at the end of every IPv4 ACP. Specifying a **discard list** is unnecessary in most applications and should be used with caution. A **discard list** can adversely affect certain functions of a unit (virtual private network (VPN), routing protocols, etc.). Specifying an empty IPv4 ACL or a nonexistent IPv4 ACL in an IPv4 ACP will result in an implicit permit.*

Usage Examples

The following example configures the IPv4 ACP **PRIVATE** using an undefined IPv4 ACL that matches all traffic, specifies the NAT pool **POOL1**, and specifies that the traffic matching this entry should be destined for the **PUBLIC** policy class:

(config)**#ip policy-class PRIVATE**
(config-policy-class)**#nat source list MATCHALL pool POOL1 policy PUBLIC**

IPv6 Access Control List Command Set

An Internet Protocol version 6 (IPv6) access control list (ACL) is an ordered list of entries used as packet selectors by an IPv6 access control policy (ACP) in the Adtran Operating System (AOS) command line interface (CLI). ACLs and ACPs work together to regulate IPv6 traffic through the routed network.

There are two types of IPv6 ACLs in AOS: **standard** and **extended**. A **standard** IPv6 ACL allows source IPv6 address packet patterns only. An **extended** IPv6 ACL may specify patterns using most fields in the IPv6 header and the Transmission Control Protocol (TCP) header, User Datagram Protocol (UDP) header, or Internet Control Message Protocol version 6 (ICMPv6) message type or code. This configuration command set details the configuration of both standard and extended IPv6 ACLs.

IPv4 ACLs are also supported by AOS, but are explained separately in this document. Refer to IPv4 Access Control List Command Set on page 4252 for more information on configuring IPv4 ACLs.

To create a **standard** IPv6 ACL and activate the Standard IPv6 ACL Configuration mode, enter the **ipv6 access-list standard** <*ipv6 acl name*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ipv6 access-list standard MATCHALLv6
(config-std6-nacl)#
```

To create an **extended** IPv6 ACL and activate the Extended IPv6 ACL Configuration mode, enter the **ipv6 access-list extended** <*ipv6 acl name*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ipv6 access-list extended MATCHALLv6
(config-ext6-nacl)#
```

*An IPv6 ACL will remain inactive until it is assigned to an **active** IPv6 ACP. For more information on configuring and activating IPv6 ACPs, refer to the IPv6 Access Control Policy Command Set on page 4326.*

Technology Review

IPv6 ACPs and ACLs regulate traffic through the routed network. When designing your traffic flow configuration, it is important to keep the following in mind:

- An IPv6 ACL serves as a packet selector, defining exactly which packets should take the given action.
- An IPv6 ACP defines the action to take on the packets selected by the ACL.
- An IPv6 ACL is inactive until it is assigned to an active IPv6 ACP.
- An IPv6 ACP is inactive until it is assigned to an interface.

IPv6 Access Control Policies

IPv6 ACPs are used to allow or discard data for each physical interface. Each IPv6 ACP consists of an action (**allow**, **discard**) and a selector (IPv6 ACL). In a sense, the IPv6 ACPs answer the question, “What should I do?” while the IPv6 ACLs answer the question, “On which packets?”

When IPv6 packets are received on an interface with an IPv6 ACP applied, the ACP is used to determine whether the data is processed or discarded. Both IPv6 ACLs and ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed. The IPv6 ACP has an implicit **discard** at the end of the list. Typically, the most specific entries should be at the top and the most general at the bottom.

IPv6 Access Control Lists

IPv6 ACLs are used as packet selectors by IPv6 ACPs. They must be assigned to an IPv6 ACP in order to be active.

IPv6 ACPs must use an IPv6 ACL. You cannot apply an IPv4 ACL to an IPv6 ACP, or vice versa. In addition, all IPv6 ACLs and IPv6 ACPs must have a different name than any configured IPv4 ACLs or IPv4 ACPs.

IPv6 ACLs are composed of an ordered list of entries. Each entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** action is used to allow packets (meeting the specified pattern) to enter the router system. A **deny** action is used to disregard packets (that do not match the specified pattern) and proceed to the next entry on the ACP. In IPv4, packets either match a **permit** or a **deny** entry in the ACL. In IPv6, if no match is found between the packet and the match criteria, a **miss** entry is passed to the application using the ACL. Depending on the application, the **miss** can be processed differently. For example, with typical IPv6 traffic, access groups treat a **miss** as a **deny**, effectually giving a **deny any any** at the end of the IPv6 ACL. For IPv6 Neighbor Discovery (ND) protocol messages, however, access groups treat **miss** packets as a **permit,** resulting in a **permit** for ND before the end of the ACL.

The AOS provides two types of IPv6 ACLs: **standard** and **extended**. A **standard** IPv6 ACL allows source IPv6 address packet patterns only. An **extended** IPv6 ACL can specify patterns using most fields in the IPv6 header, as well as the TCP header, UDP header, or ICMPv6 message type or code.

Creating and Assigning IPv6 ACLs and ACPs

Creating IPv6 ACPs and ACLs to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of AOS using the **ipv6 firewall** command. Refer to the command *ipv6 firewall on page 1523* for more information.

Step 2:
Create an IPv6 ACP that uses a configured IPv6 ACL by issuing the **ipv6 policy-class** command. AOS IPv6 ACPs are used to allow or discard data for each physical interface. Each IPv6 ACP consists of an action (**allow**, **discard**) and a selector (IPv6 ACL). When IPv6 packets are received on an interface, the configured IPv6 ACPs are applied to determine whether the data will be processed or discarded.

Step 3:
Create an IPv6 ACL to permit or deny specified IPv6 traffic by using either the **ipv6 access-list extended** or **ipv6 access-list standard** command. Standard IPv6 ACLs match based on the source IPv6 address of the packet. Extended IPv6 ACLs match based on the source and destination of the packet. Refer to the command *ipv6 access-list extended <ipv6 acl name> on page 1500* or the command *ipv6 access-list standard <ipv6 acl name> on page 1502* for more information. Sources can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.

2. Using **host** <*ipv6 address*> to specify a single host address.

3. Using the <*ipv6 prefix/prefix-length*> to specify a source IPv6 address to match.

Step 4:
Apply the created IPv6 ACP to an interface. To assign an IPv6 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ipv6 access-policy** <*ipv6 acp name*>. The following example assigns IPv6 ACP **UNTRUSTED** to the Ethernet 0/1 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 access-policy UNTRUSTED**

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

The following are commands used to configure an **extended** IPv6 ACL. **Extended** IPv6 ACL configuration includes specifying an IPv6 ACL action, a protocol, a packet source, a source port, a packet destination, and a destination port. These commands are described in this section in alphabetical order.

deny <protocol> <source> <destination> on page 4300
deny [tcp | udp] <source> <source port> <destination> <destination port> <tcp flags> on page 4302
deny icmpv6 <source> <destination> on page 4306
permit <protocol> <source> <destination> on page 4310
permit [tcp | udp] <source> <source port> <destination> <destination port> <tcp flags> on page 4312
permit icmpv6 <source> <destination> on page 4316
remark <remark> on page 4320

The following are commands for configuring a **standard** IPv6 ACL. **Standard** IPv6 ACL configuration includes specifying an ACL action and a packet source. These commands are described in this section in alphabetical order.

deny *<protocol> <source> <destination>*

Use the **deny** command to configure the extended Internet Protocol version 6 (IPv6) access control list (ACL) to deny specified packets entry into the routing system. This command provides traffic matching based on the IPv6 header field. Use the **no** form of this command to remove the deny parameter from the IPv6 ACL. Variations of this command include:

deny *<protocol> <source> <destination>*
deny ipv6 *<source> <destination>* **fragments**

Syntax Description

<protocol>	Specifies the IPv6 data protocol **ahp**, **esp**, **gre**, or a specific protocol. Range is **0** to **255**. The keyword **ipv6** can optionally be used to match any IPv6 traffic. Extension header values are not allowed.
<source>	Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** *<ipv6 address>* to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using *<ipv6 prefix/prefix-length>* to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<destination>	Specifies the destination used for IPv6 packet matching. Destinations can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** *<ipv6 address>* to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using *<ipv6 prefix/prefix-length>* to specify a destination address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
fragments	Optional. Indicates that the ACL entry is only matched by non-initial fragments. This parameter is only available using the **ipv6** protocol.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.
Release R11.10.2	Command was expanded to include the **fragments** parameter.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

IPv6 ACLs match non-initial fragments in the following manner:

- Non-initial fragments can match entries with the **fragments** keyword, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments can match entries with the **ipv6** protocol specified, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments are implicitly permitted by access groups if the fragments did not match an explicit entry in the ACL.

Usage Examples

The following example creates an entry in the **Untrustedv6** IPv6 ACL that denies IPv6 traffic matching source IPv6 prefix **2001:DB8:3F::/64** and any destination IPv6 address:

(config)**#ipv6 access-list extended Untrustedv6**
(config-ext6-nacl)**#deny ipv6** 2001:DB8:3F::/64 any

deny [tcp | udp] <*source*> <*source port*> <*destination*> <*destination port*> <*tcp flags*>

Use the **deny [tcp | udp]** command to configure the extended Internet Protocol version 6 (IPv6) access control list (ACL) to deny specified Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets entry into the routing system. This command provides traffic matching based on the IPv6 header field and the upper layer protocol flags (TCP or UDP). Use the **no** form of this command to remove the deny parameter from the IPv6 ACL. Variations of this command include:

deny tcp <*source*> <*destination*>
deny tcp <*source*> <*source port*> <*destination*>
deny tcp <*source*> <*source port*> <*destination*> <*destination port*>
deny tcp <*source*> <*source port*> <*destination*> <*destination port*> <*tcp flags*>
deny udp <*source*> <*destination*>
deny udp <*source*> <*source port*> <*destination*>
deny udp <*source*> <*source port*> <*destination*> <*destination port*>

Syntax Description

tcp	Specifies the IPv6 data protocol as TCP, indicating that TCP upper-layer protocol headers and fields are used for matching in this ACL entry.
udp	Specifies the IPv6 data protocol as UDP, indicating that UDP upper-layer protocol headers and fields are used for matching in this ACL entry.
<*source*>	Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using <*ipv6 prefix/prefix-length*> to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<*source port*>	Optional. Specifies that traffic comparison is conducted on the source port for the associated protocol (TCP or UDP). When you specify a source port, you must enter a port operator and a port number or name. The following keywords and port numbers/names are supported for the <*source port*> field:

any	Matches any destination port.
eq <*port number/name*>	Matches only packets equal to specified port number.
gt <*port number/name*>	Matches only packets with a port number greater than the specified port number.
lt <*port number/name*>	Matches only packets with a port number less than the specified port number.

neq <*port number/name*>	Matches only packets that are not equal to the specified port number.
range <*beginning port number/name*> <*ending port number/name*>	Matches only packets that contain a port number in the specified range.
<*port number*>	Specifies the port number used by TCP or UDP to pass information to upper layers using the following syntax: <***0-65535***>. All ports below 1024 are considered well-known ports, and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above 1024 are dynamically assigned ports that include registered ports for vendor-specific applications.
<*port name*>	The following UDP port numbers can be specified using the associated names:

biff (Port 512)**ntp** (Port 123)

bootpc (Port 68)	**pim-auto-rp** (Port 496)
bootps (Port 67)	**rip** (Port 520)
discard (Port 9)	**snmp** (Port 161)
dnsix (Port 195)	**snmptrap** (Port 162)
domain (Port 53)	**sunrpc** (Port 111)
echo (Port 7)	**syslog** (Port 514)
isakmp (Port 500)	**tacacs** (Port 49)
mobile-ip (Port 434)	**talk** (Port 517)
nameserver (Port 42)	**tftp** (Port 69)
netbios-dgm (Port 138)	**time** (Port 37)
netbios-ns (Port 137)	**who** (Port 513)
netbios-ss (Port 139)	**xdmcp** (Port 177)

The following TCP port numbers can be specified using the associated names:

bgp (Port 179)	**lpd** (Port 515)
chargen (Port 19)	**nntp** (Port 119)
cmd (Port 514)	**pim-auto-rp** (Port 496)
daytime (Port 13)	**pop2** (Port 109)
discard (Port 9)	**pop3** (Port 110)
domain (Port 53)	**smtp** (Port 25)
echo (Port 7)	**sunrpc** (Port 111)
exec (Port 512)	**tacacs** (Port 49)
finger (Port 79)	**talk** (Port 517)
ftp (Port 21)	**tftp** (Port 69)

gopher (Port 70)	**telnet** (Port 23)
hostname (Port 101)	**time** (Port 37)
ident (Port 113)	**uucp** (Port 540)
irc (Port 194)	**whois** (Port 43)
klogin (Port 543)	**www** (Port 80)
kshell (Port 544)	
login (Port 513)	

<destination> Specifies the destination used for IPv6 packet matching. Destinations can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.
2. Using **host** *<ipv6 address>* to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
3. Using *<ipv6 prefix/prefix-length>* to specify a destination address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

<destination port> Optional. Specifies that traffic comparison is conducted on the destination port for the associated protocol (TCP or UDP).The same keywords and port numbers/names used for the *<source port>* field are valid for the *<destination port>* field. Refer to previously listed *<source port>* for more details.

<tcp flags> Optional. When used with the TCP protocol, this option defines which flag in the TCP flag to use for traffic matching. The following keywords are the supported TCP flags:

ack	Matches the TCP acknowledgement header flag.
fin	Matches the TCP finish header flag.
psh	Matches the TCP push header flag.
rst	Matches the TCP reset header flag.
syn	Matches the TCP synchronize header flag.
urg	Matches the TCP urgent pointer header flag.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an entry in the **Untrustedv6** IPv6 ACL that denies IPv6 traffic matching TCP source IPv6 prefix **2001:DB8:3F::/64** from port **1080** and any destination IPv6 address:

(config)**#ipv6 access-list extended Untrustedv6**
(config-ext6-nacl)**#deny tcp ipv6 2001:DB8:3F::/64 eq 1080 any**

deny icmpv6 <*source*> <*destination*>

Use the **deny icmpv6** command to configure the extended Internet Protocol version 6 (IPv6) access control list (ACL) to deny specified Internet Control Message Protocol version 6 (ICMPv6) packets entry into the routing system. This command provides traffic matching based on the packet's IPv6 header field and ICMPv6-specific fields. Use the **no** form of this command to remove the deny parameter from the IPv6 ACL. Variations of this command include:

deny icmpv6 <*source*> <*destination*>
deny icmpv6 <*source*> <*destination*> <*message name*>
deny icmpv6 <*source*> <*destination*> <*message type*> <*message code*>

Syntax Description

<*source*>

Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.
2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
3. Using <*ipv6 prefix/prefix-length*> to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

<*destination*>

Specifies the destination used for IPv6 packet matching. Destinations can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.
2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
3. Using <*ipv6 prefix/prefix-length*> to specify a destination address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

<*message name*>

Optional. Specifies the ICMP message type used for matching ICMPv6 packets. ICMP message names are specified using one of the following keywords:

beyond-scope	Indicates the destination is unreachable because it is beyond the scope of the source address.
dest-unreachable	Indicates the destination address is unreachable.
dhaad-reply	Indicates a home agent address discovery reply message.

dhaad-request	Indicates a home agent address discovery request message.
echo-reply	Indicates an echo reply message.
echo-request	Indicates an echo request message.
header	Indicates an erroneous header field has been encountered.
hop-limit	Indicates the hop limit has been exceeded in packet transit.
mld-query	Indicates a mulitcast listener discovery query message.
mld-reduction	Indicates a multicast listener discovery reduction message.
mld-report	Indicates a multicast listener discovery report message.
mp-advertisement	Indicates a mobile prefix advertisement message.
mp-solicitation	Indicates a mobile prefix solicitation message.
nd-na	Indicates a Neighbor Discovery neighbor advertisement message.
nd-ns	Indicates a Neighbor Discovery neighbor solicitation message.
next-header	Indicates an unrecognized next header type was encountered.
no-admin	Indicates the destination is unreachable because communication with the destination is administratively prohibited.
no-route	Indicates the destination is unreachable because there is no route to the destination.
packet-too-big	Indicates the packet is too large.
parameter-option	Indicates that an unrecognized IPv6 option was encountered.
parameter-problem	Indicates there is a parameter problem with the packet.
port-unreachable	Indicates the destination is unreachable because the port is unreachable.

reassembly-timeout	Indicates that the fragment reassembly time limit has been exceeded.
redirect	Indicates a redirect message.
renum-command	Indicates a router renumbering command.
renum-result	Indicates a router renumbering result.
renum-seq-number	Indicates a router sequence number reset.
router-advertisement	Indicates a router advertisement message.
router-renumbering	Indicates a router renumbering for all codes.
router-solicitation	Indicates an router solicitation message.
time-exceeded	Indicates the time limit has been exceeded.
unreachable	Indicates the destination is unreachable.

<message type>	Optional. Specifies the ICMP message type for matching ICMPv6 packets. When you specify an ICMP message type, you must also specify an ICMP message code. Message types range from **0** to **127** for error messages and from **128** to **255** for informational messages.
<message code>	Optional. Specifies the ICMP message code for matching ICMPv6 packets. You must specify the message code when you specify the ICMP message type. Message code range is **0** to **255**.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an extended IPv6 ACL named **Untrustedv6** IPv6 ACL that denies any IPv6 traffic from a source with the same prefix bits as **2001:DB8:3F::/64**, headed to a destination of **2001:DB8:85A3::8A2E:0370:7334**, and an ICMPv6 message type of **echo-request**:

(config)**#ipv6 access-list extended Untrustedv6**
(config-ext6-nacl)**#deny icmpv6 2001:DB8:3F::/64 2001:DB8:85A3::8A2E:0370:7334 echo-request**

permit *<protocol> <source> <destination>*

Use the **permit** command to configure the extended Internet Protocol version 6 (IPv6) access control list (ACL) to permit specified packets entry into the routing system. This command provides traffic matching based on the IPv6 header field. Use the **no** form of this command to remove the deny parameter from the IPv6 ACL. Variations of this command include:

permit *<protocol> <source> <destination>*
permit ipv6 *<source> <destination>* **fragments**

Syntax Description

<protocol>	Specifies the IPv6 data protocol **ahp**, **esp**, **gre**, or a specific protocol. The keyword **ipv6** can optionally be used to match any IPv6 traffic. Range is **0** to **255**. Extension header values are not allowed.
<source>	Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** *<ipv6 address>* to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using *<ipv6 prefix/prefix-length>* to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<destination>	Specifies the destination used for IPv6 packet matching. Destinations can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** *<ipv6 address>* to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using *<ipv6 prefix/prefix-length>* to specify a destination address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
fragments	Optional. Indicates that the ACL entry is only matched by non-initial fragments. This parameter is only available using the **ipv6** protocol.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.
Release R11.10.2	Command was expanded to include the **fragments** parameter.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

IPv6 ACLs match non-initial fragments in the following manner:

- Non-initial fragments can match entries with the **fragments** keyword, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments can match entries with the **ipv6** protocol specified, provided the other Layer 3 information specified in the entry matches the packet.
- Non-initial fragments are implicitly permitted by access groups if the fragments did not match an explicit entry in the ACL.

Usage Examples

The following example creates an entry in the **Untrustedv6** IPv6 ACL that permits IPv6 traffic matching source IPv6 prefix **2001:DB8:3F::/64** and any destination IPv6 address:

(config)**#ipv6 access-list extended Untrustedv6**
(config-ext6-nacl)**#permit ipv6** 2001:DB8:3F::/64 any

permit [tcp | udp] <*source*> <*source port*> <*destination*> <*destination port*> <*tcp flags*>

Use the **permit [tcp | udp]** command to configure the extended Internet Protocol version 6 (IPv6) access control list (ACL) to permit specified Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets entry into the routing system. This command provides traffic matching based on the IPv6 header field and the upper layer protocol flags (TCP or UDP). Use the **no** form of this command to remove the deny parameter from the IPv6 ACL. Variations of this command include:

permit tcp <*source*> <*destination*>
permit tcp <*source*> <*source port*> <*destination*>
permit tcp <*source*> <*source port*> <*destination*> <*destination port*>
permit tcp <*source*> <*source port*> <*destination*> <*destination port*> <*tcp flags*>
permit udp <*source*> <*destination*>
permit udp <*source*> <*source port*> <*destination*>
permit udp <*source*> <*source port*> <*destination*> <*destination port*>

Syntax Description

tcp	Specifies the IPv6 data protocol as TCP, indicating that TCP upper-layer protocol headers and fields are used for matching in this ACL entry.
udp	Specifies the IPv6 data protocol as UDP, indicating that UDP upper-layer protocol headers and fields are used for matching in this ACL entry.
<*source*>	Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using <*ipv6 prefix/prefix-length*> to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<*source port*>	Optional. Specifies that traffic comparison is conducted on the source port for the associated protocol (TCP or UDP). When you specify a source port, you must enter a port operator and a port number or name. The following keywords and port numbers/names are supported for the <*source port*> field:

any	Matches any destination port.
eq <*port number/name*>	Matches only packets equal to specified port number.
gt <*port number/name*>	Matches only packets with a port number greater than the specified port number.
lt <*port number/name*>	Matches only packets with a port number less than the specified port number.

neq *<port number/name>* — Matches only packets that are not equal to the specified port number.

range *<beginning port number/name>* *<ending port number/name>* — Matches only packets that contain a port number in the specified range.

<port number> — Specifies the port number used by TCP or UDP to pass information to upper layers using the following syntax: <***0-65535***>. All ports below 1024 are considered well-known ports, and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above 1024 are dynamically assigned ports that include registered ports for vendor-specific applications.

<port name> — The following UDP port numbers can be specified using the associated names:

biff (Port 512)	**ntp** (Port 123)
bootpc (Port 68)	**pim-auto-rp** (Port 496)
bootps (Port 67)	**rip** (Port 520)
discard (Port 9)	**snmp** (Port 161)
dnsix (Port 195)	**snmptrap** (Port 162)
domain (Port 53)	**sunrpc** (Port 111)
echo (Port 7)	**syslog** (Port 514)
isakmp (Port 500)	**tacacs** (Port 49)
mobile-ip (Port 434)	**talk** (Port 517)
nameserver (Port 42)	**tftp** (Port 69)
netbios-dgm (Port 138)	**time** (Port 37)
netbios-ns (Port 137)	**who** (Port 513)
netbios-ss (Port 139)	**xdmcp** (Port 177)

The following TCP port numbers can be specified using the associated names:

bgp (Port 179)	**lpd** (Port 515)
chargen (Port 19)	**nntp** (Port 119)
cmd (Port 514)	**pim-auto-rp** (Port 496)
daytime (Port 13)	**pop2** (Port 109)
discard (Port 9)	**pop3** (Port 110)
domain (Port 53)	**smtp** (Port 25)
echo (Port 7)	**sunrpc** (Port 111)
exec (Port 512)	**tacacs** (Port 49)
finger (Port 79)	**talk** (Port 517)
ftp (Port 21)	**tftp** (Port 69)

gopher (Port 70)	**telnet** (Port 23)
hostname (Port 101)	**time** (Port 37)
ident (Port 113)	**uucp** (Port 540)
irc (Port 194)	**whois** (Port 43)
klogin (Port 543)	**www** (Port 80)
kshell (Port 544)	
login (Port 513)	

<destination> Specifies the destination used for IPv6 packet matching. Destinations can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.
2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
3. Using <*ipv6 prefix/prefix-length*> to specify a destination address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

<destination port> Optional. Specifies that traffic comparison is conducted on the destination port for the associated protocol (TCP or UDP).The same keywords and port numbers/names used for the <*source port*> field are valid for the <*destination port*> field. Refer to previously listed <*source port*> for more details.

<tcp flags> Optional. When used with the TCP protocol, this option defines which flag in the TCP flag to use for traffic matching. The following keywords are the supported TCP flags:

ack	Matches the TCP acknowledgement header flag.
fin	Matches the TCP finish header flag.
psh	Matches the TCP push header flag.
rst	Matches the TCP reset header flag.
syn	Matches the TCP synchronize header flag.
urg	Matches the TCP urgent pointer header flag.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an entry in the **Untrustedv6** IPv6 ACL that permits IPv6 traffic matching TCP source IPv6 prefix **2001:DB8:3F::/64** from port **1080** and any destination IPv6 address:

(config)**#ipv6 access-list extended Untrustedv6**
(config-ext6-nacl)**#permit tcp ipv6 2001:DB8:3F::/64 eq 1080 any**

permit icmpv6 <*source*> <*destination*>

Use the **permit icmpv6** command to configure the extended Internet Protocol version 6 (IPv6) access control list (ACL) to permit specified Internet Control Message Protocol version 6 (ICMPv6) packets entry into the routing system. This command provides traffic matching based on the packet's IPv6 header field and ICMPv6 specific fields. Use the **no** form of this command to remove the deny parameter from the IPv6 ACL. Variations of this command include:

permit icmpv6 <*source*> <*destination*>
permit icmpv6 <*source*> <*destination*> <*message name*>
permit icmpv6 <*source*> <*destination*> <*message type*> <*message code*>

Syntax Description

<*source*>

Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.
2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
3. Using <*ipv6 prefix/prefix-length*> to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

<*destination*>

Specifies the destination used for IPv6 packet matching. Destinations can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.
2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
3. Using <*ipv6 prefix/prefix-length*> to specify a destination address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

<*icmp message name*>

Optional. Specifies the ICMP message type used for matching ICMPv6 packets. ICMP message names are specified using one of the following keywords:

beyond-scope	Indicates the destination is unreachable because it is beyond the scope of the source address.
dest-unreachable	Indicates the destination address is unreachable.
dhaad-reply	Indicates a home agent address discovery reply message.

dhaad-request	Indicates a home agent address discovery request message.
echo-reply	Indicates an echo reply message.
echo-request	Indicates an echo request message.
header	Indicates an erroneous header field has been encountered.
hop-limit	Indicates the hop limit has been exceeded in packet transit.
mld-query	Indicates a mulitcast listener discovery query message.
mld-reduction	Indicates a multicast listener discovery reduction message.
mld-report	Indicates a multicast listener discovery report message.
mp-advertisement	Indicates a mobile prefix advertisement message.
mp-solicitation	Indicates a mobile prefix solicitation message.
nd-na	Indicates a Neighbor Discovery neighbor advertisement message.
nd-ns	Indicates an Neighbor Discovery neighbor solicitation message.
next-header	Indicates an unrecognized next header type was encountered.
no-admin	Indicates the destination is unreachable because communication with the destination is administratively prohibited.
no-route	Indicates the destination is unreachable because there is no route to the destination.
packet-too-big	Indicates the packet is too large.
parameter-option	Indicates that an unrecognized IPv6 option was encountered.
parameter-problem	Indicates there is a parameter problem with the packet.
port-unreachable	Indicates the destination is unreachable because the port is unreachable.

reassembly-timeout	Indicates that the fragment reassembly time limit has been exceeded.
redirect	Indicates a redirect message.
renum-command	Indicates a router renumbering command.
renum-result	Indicates a router renumbering result.
renum-seq-number	Indicates a router sequence number reset.
router-advertisement	Indicates a router advertisement message.
router-renumbering	Indicates a router renumbering for all codes.
router-solicitation	Indicates an router solicitation message.
time-exceeded	Indicates the time limit has been exceeded.
unreachable	Indicates the destination is unreachable.

<message type> Optional. Specifies the ICMP message type for matching ICMPv6 packets. When you specify an ICMP message type, you must also specify an ICMP message code. Message types range from **0** to **127** for error messages and from **128** to **255** for informational messages.

<message code> Optional. Specifies the ICMP message code for matching ICMPv6 packets. You must specify the message code when you specify the ICMP message type. Message code range is **0** to **255**.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an extended IPv6 ACL named **Untrustedv6** that permits any IPv6 traffic from a source with the same prefix bits as **2001:DB8:3F::/64**, headed to a destination of **2001:DB8:85A3::8A2E:0370:7334**, and an ICMPv6 message type of **echo-request**:

(config)**#ipv6 access-list extended Untrustedv6**
(config-ext6-nacl)**#permit icmpv6 2001:DB8:3F::/64 2001:DB8:85A3::8A2E:0370:7334 echo-request**

remark *<remark>*

Use the **remark** command to associate a descriptive tag with an extended Internet Protocol version 6 (IPv6) access control list (ACL). Use the **no** form of this command to remove the descriptive tag.

Syntax Description

<remark>	Specifies a descriptive tag for the ACL. Tags can be up to **80** alphanumeric characters enclosed in quotation marks. For example, “This list blocks all outbound Web traffic.”

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies a description for extended IPv6 ACL **matchall**:

(config)**#ipv6 access-list extended matchall**
(config-ext6-nacl)**#remark “Allows all ip traffic from remote location.”**

deny *<source>*

Use the **deny** command to configure the Internet Protocol version 6 (IPv6) standard access control list (ACL) to deny specified packets entry into the routing system. Use the **no** form of this command to remove the permit permission from the ACL.

Syntax Description

<source>	Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** *<ipv6 address>* to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using *<ipv6 prefix/prefix-length>* to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an IPv6 ACL **Untrusted** to deny all traffic from a source with the same prefix bits as **2001:DB8:3F::/48**:

(config)**#ipv6 access-list standard Untrusted**
(config-std6-nacl)**#deny 2001:DB8:3F::/48**

permit <*source*>

Use the **permit** command to configure the Internet Protocol version 6 (IPv6) standard access control list (ACL) to permit specified packets entry into the routing system. Use the **no** form of this command to remove the permit permission from the ACL.

Syntax Description

<*source*>	Specifies the source used for IPv6 packet matching. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any IPv6 address. 2. Using **host** <*ipv6 address*> to specify a single host address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**. 3. Using <*ipv6 prefix/prefix-length*> to specify a source address to match. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Functional Notes

IPv6 ACLs are used as packet selectors by different AOS features (firewall, virtual private network (VPN), quality of service (QoS)); by themselves they do nothing. IPv6 ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An IPv6 ACL entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to match packets (meeting the specified pattern) and allow them to enter the router system or specify that the feature using the ACL should apply its action to this traffic. A **deny** ACL advances AOS to the next ACP entry, discards the traffic, or specifies that the feature using the ACL should not apply its action to this traffic. AOS provides two types of IPv6 ACLs: standard and extended. Standard IPv6 ACLs match based on the source of the packet. Extended IPv6 ACLs match based on the source and destination of the packet.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the more general at the bottom.

Usage Examples

The following example creates an IPv6 ACL **Trusted** to permit all traffic from a source with the same prefix bits as **2001:DB8:3F::/48**:

(config)**#ipv6 access-list standard Trusted**
(config-std6-nacl)**#permit 2001:DB8:3F::/48**

remark *<remark>*

Use the **remark** command to associate a descriptive tag with a standard Internet Protocol version 6 (IPv6) access control list (ACL). Use the **no** form of this command to remove the descriptive tag.

Syntax Description

<remark>	Specifies a descriptive tag for the ACL. Tags can be up to **80** alphanumeric characters enclosed in quotation marks. For example, “This list blocks all outbound Web traffic.”

Default Values

By default, all AOS IPv6 security features are disabled, and there are no configured IPv6 ACLs.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example specifies a description for standard IPv6 ACL **matchall**:

(config)**#ipv6 access-list standard matchall**
(config-std6-nacl)**#remark “Allows all ip traffic from remote location.”**

IPv6 Access Control Policy Command Set

An Internet Protocol version 6 (IPv6) access control policy (ACP) defines a policy class containing IPv6 access control lists (ACLs) in the Adtran Operating System (AOS) command line interface (CLI). The ACP is a named policy with multiple action entries.

IPv4 ACPs are also supported by AOS, but are explained separately in this document. Refer to *IPv4 Access Control Policy Command Set on page 4278* for more information on configuring IPv4 ACPs.

To create an IPv6 ACP and activate the IPv6 Access Control Policy Configuration mode, enter the **ipv6 policy-class** <*ipv6 acp name*> command at the Global Configuration mode prompt. For example:

```
>enable
#config terminal
(config)#ipv6 policy-class PRIVATE
(config-policy6-class)#
```

> NOTE *Configured IPv6 ACPs will only be active if the **ipv6 firewall** command has been entered at the Global Configuration mode prompt to enable the AOS IPv6 security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

> CAUTION *Before applying an IPv6 ACP to an interface, verify your Telnet or secure shell (SSH) connection will not be affected by the policy. If an IPv6 ACP is applied to the interface you are connecting through and it does not allow Telnet or SSH traffic, your connection will be lost.*

Technology Review

IPv6 ACPs and ACLs regulate traffic through the routed network. When designing your traffic flow configuration, it is important to keep the following in mind:

- An IPv6 ACL serves as a packet selector, defining exactly which packets should take the given action.
- An IPv6 ACP defines the action to take on the packets selected by the ACL.
- An IPv6 ACL is inactive until it is assigned to an active IPv6 ACP.
- An IPv6 ACP is inactive until it is assigned to an interface.

IPv6 Access Control Policies

IPv6 ACPs are used to allow or discard data for each physical interface. Each IPv6 ACP consists of an action (**allow**, **discard**) and a selector (IPv6 ACL). In a sense, the IPv6 ACPs answer the question, “What should I do?” while the IPv6 ACLs answer the question, “On which packets?”

When IPv6 packets are received on an interface with an IPv6 ACP applied, the ACP is used to determine whether the data is processed or discarded. Both IPv6 ACLs and ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed. The IPv6 ACP has an implicit **discard** at the end of the list. Typically, the most specific entries should be at the top and the most general at the bottom.

IPv6 Access Control Lists

IPv6 ACLs are used as packet selectors by IPv6 ACPs. They must be assigned to an IPv6 ACP in order to be active.

IPv6 ACPs must use an IPv6 ACL. You cannot apply an IPv4 ACL to an IPv6 ACP, or vice versa. In addition, all IPv6 ACLs and IPv6 ACPs must have a different name than any configured IPv4 ACLs or ACPs.

IPv6 ACLs are composed of an ordered list of entries. Each entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** action is used to allow packets (meeting the specified pattern) to enter the router system. A **deny** action is used to disregard packets (that do not match the pattern) and proceed to the next entry on the ACP. In IPv4, packets either match a **permit** or a deny entry in the ACL. In IPv6, if no match is found between the packet and the match criteria, a **miss** entry is passed to the application using the ACL. Depending on the application, the **miss** can be processed differently. For example, with typical IPv6 traffic, access groups treat a **miss** as a **deny**, effectually giving a **deny any any** at the end of the IPv6 ACL. For IPv6 Neighbor Discovery (ND) messages, however, access groups treat **miss** packets as a **permit,** resulting in a **permit** for ND before the end of the ACL.

The AOS provides two types of IPv6 ACLs: **standard** and **extended**. A **standard** IPv6 ACL allows source IPv6 address packet patterns only. An **extended** IPv6 ACL may specify patterns using most fields in the IPv6 header and the Transmission Control Protocol (TCP) header, User Datagram Protocol (UDP) header, or Internet Control Message Protocol version 6 (ICMPv6) message type or code.

Creating and Assigning IPv6 ACLs and ACPs

Creating IPv6 ACPs and ACLs to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of AOS using the **ipv6 firewall** command. Refer to the command *ipv6 firewall on page 1523* for more information.

Step 2:
Create an IPv6 ACP that uses a configured IPv6 ACL by issuing the **ipv6 policy-class** command. Refer to the command *ipv6 policy-class <ipv6 acp name> on page 1549* for more information. AOS IPv6 ACPs are used to allow or discard data for each physical interface. Each IPv6 ACP consists of an action (**allow**, **discard**) and a selector (IPv6 ACL). When IPv6 packets are received on an interface, the configured IPv6 ACPs are applied to determine whether the data will be processed or discarded. Up to 20 IPv6 ACPs can be created.

Step 3:
Create an IPv6 ACL to permit or deny specified IPv6 traffic by using either the **ipv6 access-list extended** or **ipv6 access-list standard** command. Standard IPv6 ACLs match based on the source IPv6 address of the packet. Extended IPv6 ACLs match based on the source and destination of the packet. Refer to the command *ipv6 access-list extended <ipv6 acl name> on page 1500* or the command *ipv6 access-list standard <ipv6 acl name> on page 1502* for more information. Sources can be expressed in one of three ways:

1. Using the keyword **any** to match any IPv6 address.
2. Using **host** <*ipv6 address*> to specify a single host address.
3. Using the <*ipv6-prefix/prefix-length*> to specify a source IPv6 address to match.

Step 4:
Apply the created IPv6 ACP to an interface. To assign an IPv6 ACP to an interface, enter the interface configuration mode for the desired interface and enter **ipv6 access-policy** <*ipv6 acp name*>. The following example assigns IPv6 ACP **UNTRUSTED** to the Ethernet 0/1 interface:

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ipv6 access-policy UNTRUSTED**

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

allow list on page 4329
allow reverse list on page 4331
discard list on page 4333

allow list

Use the **allow list** command to specify an Internet Protocol version 6 (IPv6) access control list (ACL) to determine which packets are allowed to enter the interface to which the IPv6 access control policy (ACP) is assigned, and create a firewall association in the IPv6 firewall. All associations created by the **allow list** command are subject to the built-in firewall timers. Variations of this command include:

allow list <*ipv6 acl name*>
allow list <*ipv6 acl name*> **policy** <*ipv6 acp name*>
allow list <*ipv6 acl name*> **policy** <*ipv6 acp name*> **stateless**
allow list <*ipv6 acl name*> **self**
allow list <*ipv6 acl name*> **self stateless**
allow list <*ipv6 acl name*> **stateless**

Syntax Description

<*ipv6 acl name*>	Specifies the IPv6 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the IPv6 ACL will be processed by the next IPv6 ACP entry or implicitly discarded if no further ACP entries exist.
policy <*ipv6 acp name*>	Optional. Specifies the destination IPv6 ACP against which to match traffic. The IPv6 firewall attempts to match the specified ACP with the ACP that is applied to the packet's egress interface as determined by the routing table. If there is a match, the firewall attempts to match the ACL next. If there is no match, the firewall will process the packet based on the next ACP entry or implicitly discard it if no further ACP entries exist.
self	Optional. Allows packets to pass that are permitted by the IPv6 ACL and destined for any local interface on the unit. These packets are terminated by the unit and are not routed or forwarded to other destinations. Using the **self** keyword is helpful when opening up remote administrative access to the unit (Telnet, secure shell (SSH), Internet Control Message Protocol (ICMP)).
stateless	Optional. Enables bypassing of built-in firewall timers. A stateless policy session will time out, but because it does not perform stateful attack checking, a new policy session for existing connections can be easily recreated. Use for trusted traffic or traffic that the firewall is incorrectly blocking as a perceived attack.

Default Values

By default, all AOS IPv6 security features are disabled and there are no configured IPv6 ACP entries.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example configures the IPv6 ACP name **UNTRUSTED** to allow any traffic that matches the IPv6 ACL named **INWEB** to enter the router system:

(config)**#ipv6 policy-class UNTRUSTED**
(config-policy6-class)**#allow list INWEB**

allow reverse list

Use the **allow reverse list** command to specify an Internet Protocol version 6 (IPv6) access control list (ACL) to determine which packets are allowed to enter the interface to which the IPv6 access control policy (ACP) is assigned, and create a firewall association in the IPv6 firewall. The **allow reverse list** command is identical in function to the **allow list** command with the exception of the **reverse** keyword. The **reverse** keyword instructs the firewall to use the source information as the destination information and vice versa when attempting matches against the specified IPv6 ACL. Variations of this command include:

allow reverse list *<ipv6 acl name>*
allow reverse list *<ipv6 acl name>* **policy** *<ipv6 acp name>*
allow reverse list *<ipv6 acl name>* **policy** *<ipv6 acp name>* **stateless**
allow reverse list *<ipv6 acl name>* **self**
allow reverse list *<ipv6 acl name>* **self stateless**
allow reverse list *<ipv6 acl name>* **stateless**

Syntax Description

<ipv6 acl name>	Specifies the IPv6 ACL against which to check traffic before allowing packets to enter the interface. All packets not matched by the ACL will be processed by the next IPv6 ACP entry or implicitly discarded if no further ACP entries exist.
policy *<ipv6 acp name>*	Optional. Specifies the destination IPv6 ACP against which to match traffic. The firewall attempts to match the specified ACP with the ACP that is applied to the packet's egress interface as determined by the routing table. If there is a match, the firewall attempts to match the ACL next. If there is no match, the firewall will process the packet based on the next ACP entry or implicitly discard it if no further ACP entries exist.
self	Optional. Allows packets to pass that are permitted by the IPv6 ACL and destined for any local interface on the unit. These packets are terminated by the unit and are not routed or forwarded to other destinations. Using the **self** keyword is helpful when opening up remote administrative access to the unit (Telnet, secure shell (SSH), Internet Control Message Protocol (ICMP)).
stateless	Optional. Enables bypassing of built-in firewall timers. A stateless policy session will time out, but because it does not perform stateful attack checking, a new policy session for existing connections can be easily recreated. Use for trusted traffic or traffic that the firewall is incorrectly blocking as a perceived attack.

Default Values

By default, all AOS IPv6 security features are disabled and there are no configured IPv6 ACP entries.

Command History

Release 18.1	Command was introduced.

Usage Examples

The following example configures the IPv6 ACP named **UNTRUSTED** to allow any traffic that matches the IPv6 ACL named **INWEB** (with source and destination information reversed) to enter the router system:

(config)**#ipv6 policy-class UNTRUSTED**
(config-policy6-class)**#allow reverse list INWEB**

discard list

Use the **discard list** command to specify an Internet Protocol version 6 (IPv6) access control list (ACL) to determine which packets are discarded after entering the interface to which the IPv6 access control policy (ACP) is assigned. Packets matched by the IPv6 ACL will be discarded, and no further IPv6 ACP entries will be inspected. All packets not matched by the IPv6 ACL will be processed by the next ACP entry or implicitly discarded if no further ACP entries exist. Variations of this command include:

discard list <*ipv6 acl name*>
discard list <*ipv6 acl name*> **policy** <*ipv6 acp name*>
discard list <*ipv6 acl name*> **self**

Syntax Description

<*ipv6 acl name*>	Specifies the IPv6 ACL against which to check traffic before discarding the packet. All packets not matched by the IPv6 ACL will be processed by the next IPv6 ACP entry or implicitly discarded if no further ACP entries exist.
policy <*ipv6 acp name*>	Optional. Specifies the destination IPv6 ACP against which to match traffic. The firewall attempts to match the specified ACP with the ACP that is applied to the packet's egress interface as determined by the routing table. If there is a match, the firewall attempts to match the ACL next. If there is no match, the firewall will process the packet based on the next IPv6 ACP entry or implicitly discard it if no further ACP entries exist.
self	Optional. Discards packets that are matched by the IPv6 ACL and destined for any local interface on the unit. These packets, had they been allowed, would be terminated by the unit and not routed or forwarded to other destinations.

Default Values

By default, all AOS IPv6 security features are disabled and there are no configured IPv6 ACP entries.

Command History

Release 18.1	Command was introduced.

Functional Notes

AOS IPv6 ACPs are used to allow or discard IPv6 data for each physical interface. Each IPv6 ACP consists of an action (**allow**, **discard**) and a selector (IPv6 ACL). When IPv6 packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded.

*An implicit discard exists at the end of every ACP. Specifying a **discard list** is unnecessary in most applications and should be used with caution. Specifying an empty ACL or a nonexistent ACL in an ACP will result in an implicit permit.*

Usage Examples

The following example configures the IPv6 ACP named **UNTRUSTED** to discard any traffic that matches the IPv6 ACL named **INWEB**:

(config)**#ipv6 policy-class UNTRUSTED**
(config-policy6-class)**#discard list INWEB**

DHCP COMMAND SETS

This section includes the following command sets:

DHCPv4 Pool Command Set

The Dynamic Host Configuration Protocol version 4 (DHCPv4) server pool is created using the **ip dhcp pool** command from the Global Configuration mode prompt. This command creates the DHCPv4 server pool and enters the pool's configuration mode. The server pool is used to define the information to be assigned to clients by the DHCPv4 server. The pool chosen to serve a specific client's request is determined by the current pool selection algorithm. To create a DHCPv4 server pool, and enter the pool's configuration mode, enter the command as follows:

```
>enable
#configure terminal
(config)#ip dhcp pool MyPool
(config-dhcp)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

bootfile <name> on page 4338
client-identifier <identifier> on page 4339
client-name <name> on page 4340
default-router on page 4341
dns-server on page 4342
domain-name <name> on page 4343
hardware-address on page 4344
host <ipv4 address> on page 4346
lease <days> on page 4347
nap on page 4348
netbios-name-server on page 4349
netbios-node-type on page 4350
network on page 4351
next-server <ipv4 address> on page 4352
next-server-file <name> on page 4353
ntp-server <ipv4 address> on page 4354
option on page 4355

bootfile *<name>*

Use the **bootfile** command to specify a fully qualified directory-path name to a file located on a Trivial File Transfer Protocol (TFTP) server on the network. Some network devices use the file (the path sent to the Dynamic Host Configuration Protocol version 4 (DHCPv4) client in the DHCPOFFER message) for initial configuration. Use the **no** form of this command to remove a configured boot file.

Syntax Description

<name>	Specifies a fully qualified directory-path name to the file located on the network. If the file is located in the root directory of the TFTP server, enter the file name only.

Default Values

By default, there is no specified boot file.

Command History

Release 2.1	Command was introduced.

Functional Notes

RFC 2131 provides specifications for DHCPv4 servers to supply clients with information that allows the clients to exchange packets with other hosts on the network. DHCPv4 clients that do not store the correct boot software on an internal flash drive can receive a boot file from a TFTP server. The AOS DHCPv4 server can provide these devices with the address of the network TFTP server and the configuration file name. For example, some IP phones use this functionality to download the feature and key activation file. Use the command *tftp-server <name> on page 4356* to specify the IP address of the network TFTP server.

RFC 2131 includes provisions to allow DHCPv4 servers to utilize the 128 octets designated for the boot file directory-path for expanding the DHCPv4 options field. RFC 1533 outlines the available DHCPv4 variables for the options field. This process must be negotiated between client and server during the DHCPDISCOVER process and should only take place if the client specifies a small maxDHCPv4message size in the DHCPDISCOVER message.

Usage Examples

The following example specifies the location of a TFTP server on the local area network (LAN) at **10.10.0.4** and a boot file of **myconfig.cfg** (located in the TFTP server root directory) for the DHCPv4 pool **IP_Phones**:

(config)**#ip dhcp pool IP_Phones**
(config-dhcp)**#tftp sever 10.10.0.4**
(config-dhcp)**#bootfile myconfig.cfg**

client-identifier *<identifier>*

Use the **client-identifier** command to specify a unique identifier (in dotted hexadecimal notation) for a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove a configured client identifier.

Syntax Description

<identifier>	Specifies a client identifier using 7 to 28 hexadecimal characters with colon delimiters. Refer to the *Functional Notes* below for more information.

Default Values

No default values are necessary for this command.

Command History

Release 2.1	Command was introduced.

Functional Notes

DHCPv4 clients use client identifiers in place of hardware addresses. To create the client identifier, begin with the two-digit numerical code representing the media type and append the client's medium access control (MAC) address. For example, a Microsoft client with an Ethernet (01) MAC address d2:17:04:91:11:50 uses a client identifier of 01:d2:17:04:91:11:50.

Usage Examples

The following example specifies the client identifier for a Microsoft client with an Ethernet MAC address of **d217.0491.1150**:

(config)**#ip dhcp pool Microsoft_Clients**
(config-dhcp)**#client-identifier 01:d2:17:04:91:11:50**

client-name <*name*>

Use the **client-name** command to specify the name of a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured client name.

Syntax Description

<*name*>	Identifies the DHCPv4 client (example is **client1**) using an alphanumeric string (up to 32 characters in length).

The specified client name should not contain the domain name.

Default Values

By default, there are no specified client names.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a client name of **myclient**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#client-name myclient**

default-router

Use the **default-router** command to specify the default primary and secondary routers to use for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured router. Variations of this command include:

default-router *<ipv4 address>*
default-router *<ipv4 address> <secondary>*

Syntax Description

<ipv4 address>	Specifies the IPv4 address of the preferred router on the client's subnet.
<secondary>	Optional. Specifies the IPv4 address of the second preferred router on the client's subnet. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there are no specified default routers.

Command History

Release 2.1	Command was introduced.

Functional Notes

When specifying a router to use as the primary/secondary preferred router, verify that the listed router is on the same subnet as the DHCPv4 client. AOS allows a designation for two routers, listed in order of precedence.

Usage Examples

The following example configures a default router with address **192.22.4.253** and a secondary router with address **192.22.4.254**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#default-router 192.22.4.253 192.22.4.254**

dns-server

Use the **dns-server** command to specify the default Internet Protocol version 4 (IPv4) domain naming system (DNS) servers (up to four servers) to use for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured IPv4 DNS server. Variations of this command include:

dns-server <*ipv4 address*>
dns-server <*ipv4 address*> <*second*>
dns-server <*ipv4 address*> <*second*> <*third*>
dns-server <*ipv4 address*> <*second*> <*third*> <*fourth*>

Syntax Description

<*ipv4 address*>	Specifies the IPv4 address of the preferred DNS server on the network.
<*second*>	Optional. Specifies the IPv4 address of the second preferred DNS server on the network.
<*third*>	Optional. Specifies the IPv4 address of the third preferred DNS server on the network.
<*fourth*>	Optional. Specifies the IPv4 address of the fourth preferred DNS server on the network.
	IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there are no specified default DNS servers.

Command History

Release 2.1	Command was introduced.
Release 4.1	Command was expanded to include the Internet key exchange (IKE) client configuration pool.
Release 17.3	Command was expanded to include a third and fourth IPv4 DNS server listing.

Usage Examples

The following example specifies a default IPv4 DNS server with address **192.72.3.254** and a secondary DNS server with address **192.100.4.253**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#dns-server 192.72.3.254 192.100.4.253**

domain-name <*name*>

Use the **domain-name** command to specify the domain name for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured domain name.

Syntax Description

<*name*>	Identifies the DHCPv4 client (e.g., **adtran.com**) using an alphanumeric string (up to **32** characters in length).

Default Values

By default, there are no specified domain names.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a domain name of **adtran.com**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#domain-name adtran.com**

hardware-address

Use the **hardware-address** command to specify the name of a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured client name. Variations of this command include:

hardware-address <*mac address*>
hardware-address <*mac address*> <*type*>
hardware-address <*mac address*> **ethernet**
hardware-address <*mac address*> **ieee802**

Syntax Description

<*mac address*>	Specifies a valid 48-bit medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).	
<*type*>	Optional. Specifies one of the hardware types listed in RFC 1700. Valid range is **1** to **21**.	
	The valid hardware types are as follows:	
	1	10 Mb Ethernet
	2	Experimental 3 Mb Ethernet
	3	Amateur Radio AX.25
	4	Proteon ProNET Token Ring
	5	Chaos
	6	IEEE 802 Networks
	7	ARCNET
	8	Hyperchannel
	9	Lanstar
	10	Autonet Short Address
	11	LocalTalk
	12	LocalNet (IBM PCNet or SYTEK LocalNet)
	13	Ultra link
	14	SMDS
	15	Frame Relay
	16	Asynchronous Transfer Mode (ATM)
	17	High Level Data Link Control (HDLC)
	18	Fibre Channel
	19	Asynchronous Transfer Mode
	20	Serial Line
	21	Asynchronous Transfer Mode
ethernet	Optional. Specifies standard Ethernet networks.	
ieee802	Optional. Specifies IEEE 802 standard networks.	

Default Values

By default, the hardware address type is set to **10 Mbps Ethernet** (**1**).

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies an Ethernet client with a MAC address of **ae:11:54:60:99:10**:

```
(config)#ip dhcp pool MyPool
(config-dhcp)#hardware-address ae:11:54:60:99:10 ethernet
```

host *<ipv4 address>*

Use the **host** command to specify the Internet Protocol version 4 (IPv4) address and subnet mask for a manual binding to a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured client address. Variations of this command include:

host <*ipv4 address*>
host <*ipv4 address*> <*subnet mask*>

Syntax Description

<*ipv4 address*>	Specifies the IPv4 address for a manual binding to a DHCPv4 client. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Optional. Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). If the subnet mask is left unspecified, the DHCPv4 server examines its address pools to obtain an appropriate mask. If no valid mask is found in the address pools, the DHCPv4 server uses the Class A, B, or C natural mask.

Default Values

By default, there are no specified host addresses.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following examples show two different ways to specify a client with IPv4 address **12.200.5.99** and a 21-bit subnet mask:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#host 12.200.5.99 255.255.248.0**

or

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#host 12.200.5.99 /21**

lease *<days>*

Use the **lease** command to specify the duration of the lease for an Internet Protocol version 4 (IPv4) address assigned to a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to return to the default lease value. Variations of this command include:

lease *<days>*
lease *<days>* *<hours>*
lease *<days>* *<hours>* *<minutes>*

Syntax Description

<days>	Specifies the duration of the IPv4 address lease in days.
<hours>	Optional. Specifies the number of hours in a lease. You may only enter a value in the hours field if the days field is specified.
<minutes>	Optional. Specifies the number of minutes in a lease. You may only enter a value in the minutes field if the days and hours fields are specified.

Default Values

By default, an IPv4 address lease is **one** day.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a lease of **2** days:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#lease 2**

The following example specifies a lease of **1 hour**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#lease 0 1**

The following example specifies a lease of **30 minutes**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#lease 0 0 30**

nap

Use the **nap** command to enable network access protection (NAP) advertisements for the Dynamic Host Configuration Protocol version 4 (DHCPv4) server pools of AOS units that are operating as DHCPv4 servers. Use the **no** form of this command to disable NAP advertisements on the server pool.

Syntax Descriptions

No subcommands.

Default Values

By default, NAP advertisements are disabled on DHCPv4 server pools.

Command History

Release 17.8	Command was introduced.

Functional Notes

This command is used if your AOS unit is functioning as a DHCPv4 server and you want DHCPv4 server pools to advertise that they are NAP compatible because you are using desktop auditing. Desktop auditing is an AOS feature that collects NAP information through NAP messages sent in DHCPv4 messages between clients connected to the network and the network server.

Desktop auditing is configured by enabling the feature (using the command *desktop-auditing dhcp on page 1257*) and by configuring filters to limit the output of the collected NAP information. Information is limited by specifying local desktop auditing policies. The configuration of these policies is outlined in *Desktop Auditing Local Policy Command Set on page 4395*. For more information about desktop auditing, refer to the *Configuring Desktop Auditing in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables NAP advertisements on the DHCPv4 server pool **MyPool**:

```
(config)#ip dhcp pool MyPool
(config-dhcp)#nap
```

netbios-name-server

Use the **netbios-name-server** command to specify the primary and secondary network basic input/output system (NetBIOS) Windows Internet Naming Service (WINS) name servers available for use by the Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured NetBIOS name server. Variations of this command include:

netbios-name-server <*ipv4 address*>
netbios-name-server <*ipv4 address*> <*secondary*>

Syntax Description

<*ipv4 address*>	Specifies the IPv4 address of the preferred NetBIOS WINS name server on the network.
<*secondary*>	Optional. Specifies the IPv4 address of the second preferred NetBIOS WINS name server on the network. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there are no configured NetBIOS WINS name servers.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a primary NetBIOS WINS name server with an IPv4 address of **172.45.6.99** and a secondary with an IPv4 address of **172.45.8.15**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#netbios-name-server 172.45.6.99 172.45.8.15**

netbios-node-type

Use the **netbios-node-type** command to specify the type of network basic input/output system (NetBIOS) node used with Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured NetBIOS node type. Variations of this command include:

netbios-node-type <*value*>
netbios-node-type b-node
netbios-node-type h-node
netbios-node-type m-node
netbios-node-type p-node

Syntax Description

<*value*>	Specifies the NetBIOS node type using the numerical value. Refer to the node types below for the corresponding numerical values.
b-node	Specifies the broadcast node. Numeric value is **1**.
h-node	Specifies the hybrid node (recommended). Numeric value is **8**.
m-node	Specifies the mixed node. Numeric value is **4**.
p-node	Specifies the peer-to-peer node. Numeric value is **2**.

Default Values

By default, the **netbios-node-type** is set to **h-node** (hybrid node, numeric value **8**).

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a client's NetBIOS node type as **h-node**:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#netbios-node-type h-node**

Alternately, the following also specifies the client's NetBIOS node type as **h-node**:

(config-dhcp)**#netbios-node-type 8**

network

Use the **network** command to specify the subnet number and mask for an AOS Dynamic Host Configuration Protocol version 4 (DHCPv4) server address pool. Use the **no** form of this command to remove a configured subnet. Variations of this command include:

network <*ipv4 address*>
network <*ipv4 address*> <*subnet mask*>

Syntax Description

<*ipv4 address*>	Specifies the IPv4 address of the DHCPv4 address pool. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<*subnet mask*>	Optional. Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). If the subnet mask is left unspecified, the DHCPv4 server uses the Class A, B, or C natural mask.

Default Values

By default, there are no configured DHCPv4 address pools.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following examples show two different ways to configure an address pool subnet of **192.34.0.0** with a 16-bit subnet mask:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#network 192.34.0.0 255.255.0.0**

or

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#network 192.34.0.0 /16**

next-server *<ipv4 address>*

Use the **next-server** command to specify the Internet Protocol version 4 (IPv4) address presented in the server IPv4 address (SIADDR) field in the Bootstrap Protocol (BOOTP) header of the DHCPOFFER message. The next-server is generally the Trivial File Transfer Protocol (TFTP) server address that holds a boot file for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove a configured next server.

Syntax Description

<ipv4 address>	Specifies the IPv4 address presented in the SIADDR field in the BOOTP header of the DHCPOFFER message.

Default Values

By default, no next server is defined.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command specifies a different element of a DHCPOFFER message than that which is specified using the **tftp-server** command.

Usage Examples

The following example specifies the IPv4 address presented in the SIADDR field of the BOOTP header of the DHCPv4 offer packet:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#next-server 192.168.1.1**

next-server-file *<name>*

Use the **next-server-file** command to specify the file name presented in the boot file name field in the Bootstrap Protocol (BOOTP) header of the DHCPOFFER message. This file name is generally located on the next-server, the address of which is specified by the server Internet Protocol version 4 (IPv4) address (SIADDR) field presented in the BOOTP header. Use the **no** form of this command to remove a configured next server file.

Syntax Description

<file name>	Specifies the name of the file presented in the BOOTP header.

Default Values

By default, no next server file is configured.

Command History

Release 18.1	Command was introduced.

Functional Notes

This command specifies a different element of a DHCPOFFER message than that which is specified using the **bootfile** command.

Usage Examples

The following example specifies **test.cfg** as the file presented in the BOOTP header:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#next-server-file test.cfg**

ntp-server *<ipv4 address>*

Use the **ntp-server** command to specify the name of the Network Time Protocol (NTP) server published to the Dynamic Host Control Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove a defined NTP server.

Syntax Description

<ipv4 address>	Specifies the IPv4 address of the NTP server. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no NTP server is defined.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example specifies the IPv4 address of the NTP server:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#ntp-server 192.168.1.1**

option

Use the **option** command to describe a generic Dynamic Host Configuration Protocol version 4 (DHCPv4) option to be published to the client. The user can specify any number of generic options to be published to the client. Use the **no** form of this command to return to the default value. Variations of this command include:

option <*number*> **ascii** <*string*>
option <*number*> **hex** <*hexbytes*>
option <*number*> **ip** <*ipv4 address*>

Syntax Description

<*number*>	Specifies the value of the generic DHCPv4 option published to the client. Range is **0** to **255**.
ascii <*string*>	Specifies the DHCPv4 option information in simple text (ASCII) with a string of up to **256** characters.
hex <*hexbytes*>	Specifies the DHCPv4 option information as a hexadecimal number of up to **128** digits. This option requires an even number of digits.
ip <*ipv4 address*>	Specifies the DHCPv4 option information as an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no DHCPv4 options are configured.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example publishes DHCPv4 options to the client:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#option 100 ascii ascii_value**
(config-dhcp)**#option 101 hex AB458E80**
(config-dhcp)**#option 102 ip 192.168.1.1**

tftp-server *<name>*

Use the **tftp-server** command to specify the Internet Protocol version 4 (IPv4) address or IPv4 domain naming system (DNS) name of the Trivial File Transfer Protocol (TFTP) server published to the client. Use the **no** form of this command to remove a defined TFTP server.

Syntax Description

<name>	Specifies the IPv4 DNS name or dotted decimal notation IPv4 address of the server.

Default Values

By default, no TFTP server is defined.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example specifies the IPv4 address of the TFTP server:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#tftp-server 192.168.1.1**

The following example specifies the DNS name of the TFTP server:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#tftp-server MyServer.adtran.com**

timezone-offset <*value*>

Use the **timezone-offset** command to specify the time zone adjustment (in hours) published to the Dynamic Host Control Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove a time zone offset.

Syntax Description

<*value*>	Specifies the time zone adjustment (in hours) published to the client. Use an integer from **-12** to **12** hours.

Default Values

No default values are necessary for this command.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example sets the time zone adjustment for the client to **-3** hours. For example, if the server time is configured for Eastern time and the client is configured for Pacific time, you can set the client time zone adjustment to -3 hours:

(config)**#ip dhcp pool MyPool**
(config-dhcp)**#timezone-offset -3**

vrf *<name>*

Use the **vrf** command to associate a Dynamic Host Configuration Protocol version 4 (DHCPv4) address pool with a specific virtual routing and forwarding (VRF) instance. An address pool can only be assigned to one VRF instance, but a VRF instance can have multiple address pools providing addresses for it. Use the **no** form of this command to remove the association with the named VRF instance and assign the address pool to the default (unnamed) VRF instance.

Keep in mind that associating a DHCPv4 address pool with a nondefault VRF instance will clear all previously configured settings for the address pool.

Syntax Description

<name>	Specifies the name of the VRF instance to associate with the DHCPv4 address pool.

Default Values

By default, DHCPv4 address pools are associated with the default unnamed VRF instance.

Command History

Release 17.1	Command was introduced.
Release 18.3	Command was added to Border Gateway Protocol (BGP) and Dynamic Host Control Protocol (DHCP) version 4 (DHCPv4) and version 6 (DHCPv6).
Release R11.2.0	Command was added to network monitoring

Functional Notes

VRF instances must be created first before a DHCPv4 address pool can be assigned. An address pool can only be assigned to one VRF instance, but multiple address pools can be assigned to the same VRF instance.

VRF instances on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF instance will only affect the default unnamed VRF instance.

Usage Examples

The following example creates a DHCPv4 address pool named **PRIVATE** and assigns it to the VRF instance named **RED**:

(config)**#ip dhcp pool PRIVATE**
(config-dhcp)**#vrf RED**
WARNING!!! All settings for this pool have been removed
(config-dhcp)**#network 10.22.199.0 255.255.255.0**

DHCPv6 Pool Command Set

The Dynamic Host Configuration Protocol version 6 (DHCPv6) server pool is created using the **ipv6 dhcp pool** command from the Global Configuration mode prompt. This command creates the DHCPv6 server pool and enters the pool's configuration mode. The server pool is used to define the information to be assigned to clients by the DHCPv6 server. The pool chosen to serve a specific client's request is determined by the current pool selection algorithm, just as in DHCPv4. To create a DHCPv6 server pool, and enter the pool's configuration mode, enter the command as follows:

```
>enable
#configure terminal
(config)#ipv6 dhcp pool MyPool
(config-dhcpv6)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

address prefix

Use the **address prefix** command to specify an Internet Protocol version 6 (IPv6) address prefix from which the Dynamic Host Control Protocol version 6 (DHCPv6) server assigns addresses to requesting clients served by this server pool. Use the **no** form of this command to remove the IPv6 address prefix. Variations of this command include:

address prefix <*ipv6 prefix/prefix-length*>
address prefix <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> <*preferred lifetime*>
address prefix <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> **infinite**
address prefix <*ipv6 prefix/prefix-length*> **lifetime infinite** <*preferred lifetime*>
address prefix <*ipv6 prefix/prefix-length*> **lifetime infinite infinite**
address prefix <*prefix name*> <*ipv6 prefix/prefix-length*>
address prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> <*preferred lifetime*>
address prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> **infinite**
address prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite** <*preferred lifetime*>
address prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite infinite**
address prefix named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*>
address prefix named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> <*preferred lifetime*>
address prefix named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> **infinite**
address prefix named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite** <*preferred lifetime*>
address prefix named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite infinite**

Syntax Description

<*ipv6 prefix/prefix-length*>	Specifies the numerical value and length of the IPv6 address prefix. The prefix value is specified in colon hexadecimal format (**X:X::X/<Z>**), for example: **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<*prefix name*>	Specifies the name of the variable that holds the service provider assigned value for the IPv6 address prefix. The IPv6 prefix cannot be a link-local address.
named-prefix	Optional. Specifies that the address is constructed using the value defined in the named prefix. If a named prefix is used, the lifetime values are determined by the named prefix's configuration and do not need to be specified with this command.
lifetime	Optional. Specifies the lifetime of the IPv6 address prefix in the DHCPv6 server pool.
<*valid lifetime*>	Specifies the value of the valid lifetime for the IPv6 address prefix. This value must be longer than the preferred lifetime value. Valid lifetime range is **0** to **4294967295** seconds, with a default value of **2592000** seconds.
<*preferred lifetime*>	Specifies the preferred lifetime for the IPv6 address prefix. This value must be shorter than the valid lifetime value. Valid preferred lifetime range is **0** to **4294967295** seconds, with a default value of **604800** seconds.

infinite	Specifies that the prefix does not age.

Default Values

By default, no IPv6 address prefix are specified or sent to the DHCPv6 client. By default, when using a named prefix with this command, the default lifetime values are those assigned by the delegating DHCPv6 server.

Command History

Release R10.1.0	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** parameter.

Functional Notes

This command can be entered multiple times, once for each link IPv6 address. Up to 50 IPv6 prefixes can be entered.

Usage Examples

The following example specifies an IPv6 address prefix of **2001:DB8:3F::/64** is assigned to requesting DHCPv6 clients by the server pool. This IPv6 address prefix is configured with **infinite** valid and preferred lifetimes.

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#address prefix 2001:DB8:3F::/64 infinite infinite**

bootfile *<url>*

Use the **bootfile** command to specify a boot file uniform resource locator (URL) that will be supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients served by this DHCPv6 server pool. The URL is conveyed in the Bootfile URL option 59, and the requesting client can use the URL to load a boot file. Use the **no** form of this command to remove the URL from the DHCPv6 pool.

Syntax Description

<url>	Specifies the transfer protocol, the location, and the name of the boot file to be transferred to the DHCPv6 client. URLs are specified in a valid string of up to **512** characters in the following format: **protocol://path/filename.ext**.

Default Values

By default, no boot file URL is specified or sent to requesting DHCPv6 clients.

Command History

Release 18.3	Command was introduced.

Functional Notes

DHCPv6 is the Internet Protocol version 6 (IPv6) version of DHCPv4 (which works with IPv4). In DHCPv4, the Trivial File Transfer Protocol (TFTP) protocol is used, in conjunction with a name in a directory path, to specify which boot file should be used by requesting DHCP clients. In DHCPv6, however, a URL is used to specify a file location and transfer protocol for the boot file used by DHCPv6 clients.

Usage Examples

The following example specifies the URL **FTP://hostname/ftpshared/folder/filename1.ext** for requesting DHCPv6 clients:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#bootfile FTP://hostname/ftpshared/folder/filename1.ext**

client-identifier

Use the **client-identifier** command to specify the Dynamic Host Control Protocol version 6 (DHCPv6) client ID (DUID) that represents a single client and, together with the identity association identifier (IAID), identifies a single interface on a single DHCPv6 client. Use the **no** form of this command to remove the DUID from the DHCPv6 server pool. Variations of this command include:

client-identifier <*client DUID*>
client-identifier <*client DUID*> <*IAID*>

Syntax Description

<*client DUID*>	Specifies the DUID of the client to be matched. The DUID is expressed as a hexadecimal value.
<*IAID*>	Optional. Specifies a hexadecimal value that represents the IAID expected in the DHCPv6 client request. This option is useful if the client has more than one interface requesting DHCPv6 information, and specific information is required for each interface.

Default Values

By default, no DHCPv6 DUID is specified.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The value specified when using this command is used to allow a single device, or interface, to match the DHCPv6 server pool and is used as part of the automatic pool selection algorithm that matches DHCPv6 client requests to the best server pool from which to assign information to the client. When specifying this command, you should remember that a specified DUID can be present in one DHCPv6 server pool only. You can, however, create multiple DUIDs by using multiple instances of this command. Each ID is created and deleted individually. Up to 50 IDs can be created on a single DHCPv6 server pool.

Usage Examples

The following example creates the client ID (the DUID) **F2A4C9** for the requesting DHCPv6 client:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#client-identifier F2A4C9**

dns-server *<ipv6 address>*

Use the **dns-server** command to specify the Internet Protocol version 6 (IPv6) address of a domain naming system (DNS) server supplied to Dynamic Host Control Protocol version 6 (DHCPv6) requesting clients for this DHCPv6 server pool. Use the **no** version of this command to remove the DNS server address from the pool. If the **no** version of this command is entered without specifying an IPv6 address, all DNS server addresses are removed from the pool.

Syntax Description

<ipv6 address>	Specifies the IPv6 address of the DNS server for requesting DHCPv6 clients. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **20012:DB8:1::1**. Up to **50** DNS server addresses can be entered.

Default Values

By default, no DNS server address is specified or sent to the requesting DHCPv6 client.

Command History

Release 18.3	Command was introduced.

Functional Notes

Multiple DNS server addresses can be entered by using multiple instances of this command. Each address is added or deleted individually. Up to **50** DNS server addresses can be entered. These addresses are assigned in the order they are entered. If the **no** version of this command is entered without specifying an IPv6 address, all DNS server addresses are removed from the DHCPv6 pool.

Usage Examples

The following example adds a DNS server address to the DHCPv6 server pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#dns-server 2001:DB8:1::1**

domain-name <*name*>

Use the **domain-name** command to specify a domain name suffix to be supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients served by this DHCPv6 server pool. Use the **no** version of this command to remove the domain name from the pool. If the **no** version of this command is entered without specifying a domain name, all domain names are removed from the pool.

Syntax Description

<*name*>	Specifies the domain name suffix supplied to requesting DHCPv6 clients. Domain names are specified in ASCII text of up to **245** characters, and are typically a domain name suffix the client uses to fully quality host names.

Default Values

By default, no domain names are specified or sent to the requesting DHCPv6 client.

Command History

Release 18.3	Command was introduced.

Functional Notes

Multiple domain names can be entered using multiple instances of this command. Each name is added or deleted individually. Up to **50** domain names can be entered. These names are assigned in the order they are entered. If the **no** version of this command is entered without specifying a domain name, all domain names are removed from the pool.

Usage Examples

The following example adds the domain name **Name1** to the DHCPv6 pool for requesting DHCPv6 clients:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#doman-name Name1**

host client-identifier

Use the **host client-identifier** command to create a Dynamic Host Control Protocol version 6 (DHCPv6) host entry within the DHCPv6 server pool. This command creates a host entry in the server pool, and enters the DHCPv6 Host Configuration mode. The command also specifies the manual binding of a set of information to a single client as identified by a DHCPv6 client ID (DUID). Use the **no** form of this command to remove the DUID from the server pool. Variations of this command include:

host client-identifier <*client DUID*>
host client-identifier <*client DUID*> <*IAID*>

Syntax Description

<*client DUID*>	Specifies the DUID of the client to be matched as a DHCPv6 host. The DUID is expressed as a hexadecimal value.
<*IAID*>	Optional. Specifies a hexadecimal value that represents the IAID expected in the DHCPv6 client request.

Default Values

By default, no host DUID is specified.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The value specified by this command is used to allow a single device, or interface, to match the DHCPv6 server pool and is used as part of the automatic pool selection algorithm that matches DHCPv6 client requests to the best pool from which to assign information to the client.

Using this command also enters the DHCPv6 Host Configuration mode. From the Host Configuration mode, you can specify Internet Protocol version 6 (IPv6) address and hostname bindings for a single DHCPv6 client. For more information about the DHCPv6 Host Configuration mode, refer to *DHCPv6 Server Pool Host Command Set on page 4383*.

Usage Examples

The following example creates a DHCPv6 host DUID of **F2A4C9** and enters the DHCPv6 Host Configuration mode:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#host client-identifier F2A4C9**
(config-dhcpv6-host)#

import

Use the **import** command to instruct the Dynamic Host Control Protocol version 6 (DHCPv6) server to import the values of certain information from the global information pool when serving a DHCPv6 client request. These parameters are served to DHCPv6 clients using this server pool as if their values had been configured locally in the pool. Use the **no** form of this command to disable the importation of the specified information. If no parameters are specified when the **no** version of this command is issued, then all imported parameters are removed from the pool's configuration. Variations of this command include:

import dns-server
import domain-name
import ntp
import timezone

Syntax Description

dns-server	Specifies that domain naming system (DNS) server options are imported.
domain-name	Specifies that domain name options are imported.
ntp	Specifies that Network Time Protocol (NTP) options are imported.
timezone	Specifies that time zone database information is imported.

Default Values

By default, no information is imported into the DHCPv6 server pool.

Command History

Release 18.3	Command was introduced.

Functional Notes

The parameters imported from the global information pool are served to DHCPv6 clients using this server pool as if their values had been configured locally in the pool. If the imported values do not exist in the global information pool, the respective value in the importing pool behaves as if it is not configured. Once a value exists in the global configuration, the respective value in the importing pool is initialized and can be used. These options can also be configured locally using the commands *client-identifier on page 4364*, *domain-name <name> on page 4366*, *ntp address <ipv6 address> on page 4371*, *ntp domain-name <name> on page 4372*, and *timezone on page 4379*.

This command can be issued multiple times to import a separate parameter each time. If no parameters are specified when the **no** version of the command is issued, then all imported parameters are removed from the DHCPv6 pool's configuration.

Usage Examples

The following examples enables the importation of DNS server information to the DHCPv6 server pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#import dns-server**

information refresh

Use the **information refresh** command to enable the Dynamic Host Control Protocol version 6 (DHCPv6) server to send the information refresh value to requesting clients served by this DHCPv6 pool when using the stateless exchange option for configuration information. This command also specifies the information refresh rate. Use the **no** form of this command to return the refresh rate to the default value. Variations of this command include:

information refresh infinite
information refresh <*days*>
information refresh <*days*> <*hours*>
information refresh <*days*> <*hours*> <*minutes*>

Syntax Description

infinite	Specifies that there is an infinite refresh time.
<*days*>	Specifies the number of days to wait before refreshing the assigned information. Valid range is **0** to **365** days.
<*hours*>	Optional. Specifies the number of hours to wait before refreshing the assigned information. Valid range is **0** to **23** hours.
<*minutes*>	Optional. Specifies the number of minutes to wait before refreshing the assigned information. Valid range is **0** to **59** minutes.

Default Values

By default, no information refresh time is set and the DHCPv6 client should refresh every **24** hours.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example changes the information refresh rate for clients using stateless DHCPv6 to acquire configuration information to every **4** days:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#information refresh 4**

The following example changes the information refresh rate for clients using stateless DHCPv6 to acquire configuration information every **6** days and **3** hours:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#information refresh 6 3**

The following example changes the information refresh rate for clients using stateless DHCPv6 to acquire configuration information every **20** days, **12** hours, and **30** minutes:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#information refresh 20 12 30**

link-address *<ipv6 prefix/prefix-length>*

Use the **link-address** command to specify an Internet Protocol version 6 (IPv6) prefix that the Dynamic Host Control Protocol version 6 (DHCPv6) sever can use to match a received interface or relay-forwarded client request to the server pool. Use the **no** version of this command to remove the link address form the server pool. If the **no** version of this command is entered without specifying an IPv6 prefix, all link address prefixes are removed from the pool.

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the IPv6 prefix to use for matching a client request or received interface to the server pool. The prefix value is specified in colon hexadecimal format (**X:X::X/<Z>**), for example: **2001:DB8:3F::/64**.

Default Values

By default, no link addresses are specified in the DHCPv6 pool.

Command History

Release 18.3	Command was introduced.

Functional Notes

The IPv6 prefix value is only used as part of the automatic DHCPv6 pool selection that matches client requests to the pool from which to assign information to the client. The prefix is typically the prefix of the DHCPv6 relay agent's interface.

Multiple IPv6 prefixes can be entered using multiple instances of this command. Each prefix is added or deleted individually. Up to **50** IPv6 prefixes can be entered. If the **no** version of this command is entered without specifying a prefix, all link address prefixes are removed from the pool.

Usage Examples

The following example adds an IPv6 link address prefix to the DHCPv6 pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#link-address 2001:DB8:3F::/64**

ntp address *<ipv6 address>*

Use the **ntp address** command to specify the unicast Internet Protocol version 6 (IPv6) address, or a multicast group address, of a Network Time Protocol (NTP) server to be supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients served by this DHCPv6 pool. Use the **no** form of this command to remove the server address from the pool. If no NTP server address is specified when using the **no** form of this command, all NTP server addresses are removed from the pool.

Syntax Description

<ipv6 address>	Specifies the unicast or multicast IPv6 address of the NTP server to be supplied to requesting DHCPv6 clients that use this DHCPv6 pool. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.

Default Values

By default, no NTP information is specified or sent to the DHCPv6 client.

Command History

Release 18.3	Command was introduced.

Functional Notes

Multiple NTP server addresses can be entered using multiple instances of this command. Each address is added or deleted individually. Up to **50** addresses can be entered. These addresses are assigned in the order they are entered. If the **no** version of this command is entered without specifying an address, all NTP server addresses are removed from the pool.

Usage Examples

The following example adds an NTP server address to the DHCPv6 pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#ntp address 2001:DB8:1::1**

ntp domain-name *<name>*

Use the **ntp domain-name** command to specify the domain name of a Network Time Protocol (NTP) server to be supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients by this server pool. Use the **no** form of this command to remove the server domain name from the pool. If no server domain name is specified when using the **no** form of this command, all NTP server domain names are removed from the pool.

Syntax Description

<name>	Specifies the fully qualified domain name of an IPv6 NTP server.

Default Values

By default, no NTP information is specified or sent to the DHCPv6 client.

Command History

Release 18.3	Command was introduced.

Functional Notes

Multiple NTP domain names can be entered using multiple instances of this command. Each name is added or deleted individually. Up to **50** domain names can be entered. These names are assigned in the order they are entered. If the **no** version of this command is entered without specifying a domain name, all domain names are removed from the pool.

Usage Examples

The following example adds an NTP server domain name to the DHCPv6 pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#ntp domain-name Name1**

option

Use the **option** command to specify a generic Dynamic Host Control Protocol version 6 (DHCPv6) option to assign to clients using this DHCPv6 pool. Use the **no** form of this command to remove the option from the DHCPv6 pool. Variations of this command include:

option <*number*> **address** <*ipv6 address*>
option <*number*> **ascii** <*string*>
option <*number*> **hex** <*hexbytes*>

Syntax Description

<*number*>	Specifies the DHCPv6 option number. Valid range is **0** to **65535**.
address <*ipv6 address*>	Specifies the option value as an IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
ascii <*string*>	Specifies the option in simple text (ASCII) with a string of up to **256** characters.
hex <*hexbytes*>	Specifies the option value as a hexadecimal number with up to **512** digits.

Default Values

By default, no DHCPv6 options are configured.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example specifies a generic DHCPv6 option for clients using this pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#option 35 address 2001:DB8:1::1**

prefix-delegation

Use the **prefix-delegation** command to enable Internet Protocol version 6 (IPv6) address prefix delegation from the Dynamic Host Control Protocol version 6 (DHCPv6) server that assigns addresses to requesting clients served by this server pool. Use the **no** form of this command to disable IPv6 address prefix delegation. Variations of this command include:

prefix-delegation <*ipv6 prefix/prefix-length*>
prefix-delegation <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> <*preferred lifetime*>
prefix-delegation <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> **infinite**
prefix-delegation <*ipv6 prefix/prefix-length*> **lifetime infinite** <*preferred lifetime*>
prefix-delegation <*ipv6 prefix/prefix-length*> **lifetime infinite infinite**
prefix-delegation named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*>
prefix-delegation named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> <*preferred lifetime*>
prefix-delegation named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> **infinite**
prefix-delegation named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite** <*preferred lifetime*>
prefix-delegation named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite infinite**

Syntax Description

<*ipv6 prefix/prefix-length*>	Specifies the numerical value and length of the IPv6 address prefix. The prefix value is specified in colon hexadecimal format (**X:X::X/<Z>**), for example: **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
named-prefix <*prefix name*>	Optional. Specifies that the address is constructed using the value defined in the named prefix and the name of the variable that holds the service provider assigned value for the IPv6 address prefix. The IPv6 prefix cannot be a link-local address. If a named prefix is used, the lifetime values are determined by the named prefix's configuration and do not need to be specified with this command.
lifetime	Optional. Specifies the lifetime of the IPv6 address prefix in the DHCPv6 server pool.
<*valid lifetime*>	Specifies the value of the valid lifetime for the IPv6 address prefix. This value must be greater than the preferred lifetime value. Valid lifetime range is **0** to **4294967295** seconds, with a default value of **2592000** seconds.
<*preferred lifetime*>	Specifies the preferred lifetime for the IPv6 address prefix. This value must be lesse than the valid lifetime value. Valid preferred lifetime range is **0** to **4294967295** seconds, with a default value of **604800** seconds.
infinite	Specifies that the prefix does not age.

Default Values

By default, no IPv6 address prefixes are specified or sent to the DHCPv6 client. By default, when using a named prefix with this command, the default lifetime values are those assigned by the delegating DHCPv6 server.

Command History

Release R11.1.0	Command was introduced.

Usage Examples

The following example enables IPv6 address prefix delegation for requesting DHCPv6 clients served by the server pool. This IPv6 address prefix is configured with **infinite** valid and preferred lifetimes.

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#prefix-delegation 2001:DB8:3F::/64 infinite infinite**

sip address *<ipv6 address>*

Use the **sip address** command to specify the Internet Protocol version 6 (IPv6) address of a Session Initiation Protocol (SIP) server that is supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients served by this pool. Use the **no** form of this command to remove the SIP server address from the pool. If no SIP server address is specified when using the **no** form of this command, then all SIP server addresses are removed from the pool.

Syntax Description

<ipv6 address>	Specifies the SIP server address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.

Default Values

By default, no SIP server is specified or sent to the requesting DHCPv6 client.

Command History

Release 18.3	Command was introduced.

Functional Notes

Multiple server addresses can be entered using multiple instances of this command. Each address is added or deleted individually. Up to **50** addresses can be entered. These addresses are assigned in the order they are entered. If the **no** version of this command is entered without specifying an address, all SIP server addresses are removed from the pool.

Usage Examples

The following example adds a SIP server address to the DHCPv6 pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#sip address 2001:DB8:1::1**

sip domain-name <*name*>

Use the **sip domain-name** command to specify a Session Initiation Protocol (SIP) server domain name to be supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients served by this DHCPv6 pool. Use the **no** form of this command to remove the server domain name from the pool. If no server domain name is specified when using the **no** form of this command, then all SIP server domain names are removed from the pool.

Syntax Description

<*name*>	The fully qualified domain name (FQDN) of an IPv6 SIP server, entered in ASCII text of up to **256** characters.

Default Values

By default, no SIP server information is specified or sent to DHCPv6 clients.

Command History

Release 18.3	Command was introduced.

Functional Notes

Typically, the SIP server domain name is the domain name of the SIP outbound proxy server for the DHCPv6 client to use.

Multiple domain names can be entered using multiple instances of this command. Each name is added or deleted individually. Up to **50** domain names can be entered. These names are assigned in the order they are entered. If the **no** version of this command is entered without specifying a domain name, all domain names are removed from the pool.

Usage Examples

The following example adds a SIP server domain name to the DHCPv6 pool:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#sip domain-name Name1**

sntp-server *<ipv6 address>*

Use the **sntp-server** command to specify the unicast Internet Protocol version 6 (IPv6) address of a Simple Network Time Protocol (SNTP) server to be supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients served by this pool. Use the **no** form of this command to remove the server address from the pool. If no server address is specified when using the **no** form of this command, all SNTP server addresses are removed from the pool.

Syntax Description

<ipv6 address>	Specifies the IPv6 address of the SNTP server. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.

Default Values

By default, no SNTP information is specified or sent to the DHCPv6 client.

Command History

Release 18.3	Command was introduced.

Functional Notes

Multiple SNTP server addresses can be entered using multiple instances of this command. Each address is added or deleted individually. Up to **50** addresses can be entered. These addresses are assigned in the order they are entered. If the **no** version of this command is entered without specifying an address, all addresses are removed from the pool.

Usage Examples

The following example adds an SNTP server to the DHCPv6 pool:

(config)**#ipv6 dhcp pool MyPool1**
(config-dhcpv6)**#sntp-server 2001:DB8:1::1**

timezone

Use the **timezone** command to specify the time zone information that is supplied to requesting Dynamic Host Control Protocol version 6 (DHCPv6) clients served by this DHCPv6 pool. Use the **no** form of this command to remove the time zone information. Variations of this command include:

timezone <*timezone*>
timezone <*tzdb string*>
timezone posix <*string*>

Syntax Description

<*timezone*>	Specifies the time zone using a predefined value. Enter **timezone ?** to display the available time zones and their associated cities.
<*tzdb string*>	Specifies a time zone string in standard time zone (TZ) database format (as defined in RFC 4833). TZ database strings are limited to **256** characters.
posix <*string*>	Specifies a time zone in POSIX form, using the following format: **EST5EDT4,M3.2.0/02:00,M11.1.0/02:00**.

Default Values

By default, no time zone information is specified.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example specifies a time zone for requesting DHCPv6 clients using TZ database format:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#timezone America\Chicago**

vendor-specific <*number*>

Use the **vendor-specific** command to specify a specific vendor option for the Dynamic Host Control Protocol version 6 (DHCPv6) pool and to enter the vendor-specific configuration mode. Use the **no** form of this command to remove the vendor-specific options or suboptions from the pool. Variations of this command include:

vendor-specific <*number*>

Additional subcommands are available once you have entered the vendor-specific DHCPv6 Pool Configuration mode:

suboption <*number*> **address** <*ipv6 address*>
suboption <*number*> **ascii** <*string*>
suboption <*number*> **hex** <*hexbytes*>

Syntax Description

vendor-specific <*number*>	Specifies the enterprise identifier of the vendor information you are entering. Valid range is **1** to **4294967295**.
suboption <*number*>	Specifies the vendor-specific option number for the suboption. Valid range is **0** to **65535**.
address <*ipv6 address*>	Specifies that the suboption value is an IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
ascii <*string*>	Specifies that the suboption is expressed as a simple text ASCII string of up to **256** characters.
hex <*hexbytes*>	Specifies that the suboption is expressed as a hexadecimal number of up to **512** digits.

Default Values

By default, no vendor-specific options or suboptions are configured.

Command History

Release 18.3	Command was introduced.

Usage Examples

The following example configures a vendor-specific DHCPv6 pool entry, and configures a suboption for that entry:

(config)**#ipv6 dhcp pool MyPool**
(config-dhcpv6)**#vendor-specific 6**
(config-dhcpv6-vs)**#suboption 7 address 2001:DB8:1::1**

vrf *<name>*

Use the **vrf** command to associate a Dynamic Host Configuration Protocol version 6 (DHCPv4) server address pool with a specific virtual routing and forwarding (VRF) instance. An address pool can only be assigned to one VRF instance, but a VRF instance can have multiple address pools providing addresses for it. Use the **no** form of this command to remove the association with the named VRF instance and assign the address pool to the default (unnamed) VRF instance.

Keep in mind that associating a DHCPv6 address pool with a nondefault VRF instance will clear all previously configured settings for the address pool.

Syntax Description

<name>	Specifies the name of the VRF instance to associate with the DHCPv6 address pool.

Default Values

By default, DHCPv6 address pools are associated with the default unnamed VRF instance.

Command History

Release 17.1	Command was introduced.
Release 18.3	Command was added to Border Gateway Protocol (BGP) and Dynamic Host Control Protocol (DHCP) version 4 (DHCPv4) and version 6 (DHCPv6).
Release R11.2.0	Command was added to network monitoring.

Functional Notes

VRF instances must be created first before a DHCPv6 address pool can be assigned. An address pool can only be assigned to one VRF instance, but multiple address pools can be assigned to the same VRF instance.

VRF instances on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured. Therefore, executing the abovementioned commands without specifying a VRF instance will only affect the default unnamed VRF instance.

Usage Examples

The following example creates a DHCPv6 address pool named **PRIVATE** and assigns it to the VRF instance named **RED**:

(config)**#ipv6 dhcp pool PRIVATE**
(config-dhcpv6)**#vrf RED**
WARNING!!! All settings for this pool have been removed
(config-dhcpv6)**#network 10.22.199.0 255.255.255.0**

DHCPv6 Server Pool Host Command Set

In Dynamic Host Control Protocol version 6 (DHCPv6), you can create a DHCPv6 host entry within a DHCPv6 server pool by issuing the **host client-identifier** command from the DHCPv6 Server Pool Configuration mode. This command creates a host entry in the server pool and enters the DHCPv6 Server Pool Host Configuration mode. From this mode, you can specify an Internet Protocol version 6 (IPv6) address and additional host name bindings for a single DHCPv6 client.

To create a DHCPv6 host entry within a DHCPv6 server pool, enter the **host client-identifier** command from the DHCPv6 Server Pool Configuration mode as follows:

```
(config)#ipv6 dhcp pool MYPOOL
(config-dhcpv6)#host client-identifier F2A4C9
(config-dhcpv6-host)#
```

For more information about configuring DHCPv6, and DHCPv6 server pools, refer to the configuration guide *Configuring DHCPv6 in AOS* available online at http://supportforums.adtran.com and the *DHCPv6 Pool Command Set on page 4360* of this guide.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76

All other commands for this command set are described in this section in alphabetical order.

address <ipv6 address> lifetime on page 4384
host client-identifier on page 4386
hostname on page 4387
prefix-delegation on page 4388

address <*ipv6 address*> lifetime

Use the **address lifetime** command to specify an Internet Protocol version 6 (IPv6) address is manually bound to a single Dynamic Host Control Protocol version 6 (DHCPv6) client, identified by its client ID (DUID). Use the **no** form of this command to remove the IPv6 address association from the host client. Variations of this command include:

address <*ipv6 address*> **lifetime** <*valid lifetime*> <*preferred lifetime*>
address <*ipv6 address*> **lifetime** <*valid lifetime*> **infinite**
address <*ipv6 address*> **lifetime infinite** <*preferred lifetime*>
address <*ipv6 address*> **lifetime infinite infinite**
address named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> <*preferred lifetime*>
address named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime** <*valid lifetime*> **infinite**
address named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite** <*preferred lifetime*>
address named-prefix <*prefix name*> <*ipv6 prefix/prefix-length*> **lifetime infinite infinite**

Syntax Description

<*ipv6 address*>	Specifies the IPv6 address to assign to the single DHCPv6 client. There is no prefix length associated with this address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
named-prefix	Optional. Specifies that the address is constructed using the value defined in the named prefix.
<*prefix name*>	Specifies the name of the variable that holds the service provider assigned value for the IPv6 address prefix. The IPv6 prefix cannot be a link-local address.
<*ipv6 prefix/prefix-length*>	Specifies the numerical value and length of the IPv6 address prefix. The prefix value is specified in colon hexadecimal format (**X:X::X/<Z>**), for example: **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
<*valid lifetime*>	Specifies the valid lifetime of the IPv6 address. This value must be longer than the preferred lifetime value. Valid lifetime range is **0** to **4294967295** seconds. By default, the valid lifetime value is set to **2592000** seconds.
<*preferred lifetime*>	Specifies the preferred lifetime of the IPv6 address. This value must be shorter than the valid lifetime. Valid preferred lifetime range is **0** to **4294967295** seconds. By default, the preferred lifetime value is set to **604800** seconds.
infinite	Specifies that the IPv6 address does not age. This parameter can be used instead of either the valid lifetime or preferred lifetime value.

Default Values

By default, no IPv6 address is bound to a client.

Command History

Release R10.1.0	Command was introduced.
Release R10.9.0	Command was expanded to include the **named-prefix** parameter.

Functional Notes

Multiple IPv6 addresses (up to 50) can be entered for a single DUID using multiple instances of this command.

Usage Examples

The following example specifies that the IPv6 address **2001:DB8::1**, with infinite valid and preferred lifetimes, is assigned to the DHCPv6 host client **F2A4C9**:

(config-dhcpv6)**#host client-identifier F2A4C9**
(config-dhcpv6-host)**#address 2001:DB8::1 lifetime infinite infinite**

host client-identifier

Use the **host client-identifier** command to create a Dynamic Host Control Protocol version 6 (DHCPv6) host entry within the DHCPv6 Host Configuration mode. This command creates a host entry in the host server pool and specifies the manual binding of a set of information to a single client as identified by a DHCPv6 client ID (DUID). Use the **no** form of this command to remove the host client ID (DUID) from the host server pool. Variations of this command include:

host client-identifier <*client DUID*>
host client-identifier <*client DUID*> <*IAID*>

Syntax Description

<*client DUID*>	Specifies the DUID of the client to be matched as a DHCPv6 host. The DUID is expressed as a hexadecimal value.
<*IAID*>	Optional. Specifies a hexadecimal value that represents the IAID expected in the DHCPv6 client request.

Default Values

By default, no host DUID is specified.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

The value specified by this command is used to allow a single device, or interface, to match the DHCPv6 server pool host.

Usage Examples

The following example creates a DHCPv6 host DUID of **F2A4C9** in the DHCPv6 Host Configuration mode:

(config-dhcpv6)**#host client-identifier F2A4C9**
(config-dhcpv6-host)**#host client-identifier F2A4C8**

hostname

Use the **hostname** command to specify the manual binding of a host name or fully qualified domain name (FQDN) to the specified Dynamic Host Control Protocol version 6 (DHCPv6) client. Use the **no** form of this command to remove the host name or FQDN from the client. Variations of this command include:

hostname <*partial fqdn*>
hostname fqdn <*fqdn*>

Syntax Description

<*partial fqdn*>	Specifies the DHCPv6 client's host portion of its FQDN without a specified zone.
fqdn <*fqdn*>	Specifies the DHCPv6 client's entire FQDN.

Default Values

By default, no host names are specified.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example specifies an FQDN for the DHCPv6 client **F2A4C9**:

(config-dhcpv6)**#host client-identifier F2A4C9**
(config-dhcpv6-host)**#hostname fqdn host.company.com**

prefix-delegation

Use the **prefix-delegation** command to enable Internet Protocol version 6 (IPv6) address prefix delegation from the Dynamic Host Control Protocol version 6 (DHCPv6) server to a single DHCPv6 client, identified by its client ID (DUID . Use the **no** form of this command to disable IPv6 address prefix delegation. Variations of this command include:

prefix-delegation *<ipv6 prefix/prefix-length>*
prefix-delegation *<ipv6 prefix/prefix-length>* **lifetime** *<valid lifetime> <preferred lifetime>*
prefix-delegation *<ipv6 prefix/prefix-length>* **lifetime** *<valid lifetime>* **infinite**
prefix-delegation *<ipv6 prefix/prefix-length>* **lifetime infinite** *<preferred lifetime>*
prefix-delegation *<ipv6 prefix/prefix-length>* **lifetime infinite infinite**
prefix-delegation named-prefix *<prefix name> <ipv6 prefix/prefix-length>*
prefix-delegation named-prefix *<prefix name> <ipv6 prefix/prefix-length>* **lifetime** *<valid lifetime> <preferred lifetime>*
prefix-delegation named-prefix *<prefix name> <ipv6 prefix/prefix-length>* **lifetime** *<valid lifetime>* **infinite**
prefix-delegation named-prefix *<prefix name> <ipv6 prefix/prefix-length>* **lifetime infinite** *<preferred lifetime>*
prefix-delegation named-prefix *<prefix name> <ipv6 prefix/prefix-length>* **lifetime infinite infinite**

Syntax Description

<ipv6 prefix/prefix-length>	Specifies the numerical value and length of the IPv6 address prefix. The prefix value is specified in colon hexadecimal format (**X:X::X/<Z>**), for example: **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.
named-prefix *<prefix name>*	Optional. Specifies that the address is constructed using the value defined in the named prefix and the name of the variable that holds the service provider assigned value for the IPv6 address prefix. The IPv6 prefix cannot be a link-local address. If a named prefix is used, the lifetime values are determined by the named prefix's configuration and do not need to be specified with this command.
lifetime	Optional. Specifies the lifetime of the IPv6 address prefix in the DHCPv6 server pool.
<valid lifetime>	Specifies the value of the valid lifetime for the IPv6 address prefix. This value must be greater than the preferred lifetime value. Valid lifetime range is **0** to **4294967295** seconds, with a default value of **2592000** seconds.
<preferred lifetime>	Specifies the preferred lifetime for the IPv6 address prefix. This value must be less than the valid lifetime value. Valid preferred lifetime range is **0** to **4294967295** seconds, with a default value of **604800** seconds.
infinite	Specifies that the prefix does not age.

Default Values

By default, no IPv6 address prefixes are specified or sent to the DHCPv6 client. By default, when using a named prefix with this command, the default lifetime values are those assigned by the delegating DHCPv6 server.

Command History

Release R11.1.0	Command was introduced.

Usage Examples

The following example enables IPv6 address prefix delegation for requesting DHCPv6 clients served by the server pool. This IPv6 address prefix is configured with **infinite** valid and preferred lifetimes.

```
(config-dhcpv6)#host client-identifier F2A4C9
(config-dhcpv6-host)#prefix-delegation 2001:DB8:3F::/64 infinite infinite
```

SERVICES COMMAND SETS

This section includes the following command sets:

COUNTER PROFILE CONFIGURATION COMMAND SET

The Counter Profile Configuration Command Set allows you to modify a profile for a counter. The profile can then be used to define the behavior of one or more dynamic counters. Dynamic counters allow you to set up a counter that monitors traffic as it is transmitted to, or received by any interface. In addition to the interface to be monitored, the virtual local area network (VLAN), VLAN priority bit, and color of the traffic can be specified.

Counter profiles are created and configured using the counter-profile command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#counter-profile 0/1
(config-count-prof 0/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76

All other commands for this command set are described in this section in alphabetical order.

color

Use the **color** command to include color marking in the selected counter profile. Use the **no** form of this command to remove color marking from the selected counter profile. Variations of this command include:

color green
color red
color yellow

Syntax Description

green	Marks packets that comply with CIR/CBS as green.
red	Marks packets that violate CIR/CBS and EIR/EBS as red.
yellow	Marks packets that violate CIR/CBS but comply with EIR/EBS as yellow.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example marks packets that comply with CIR as ‘green’:

(config)**#counter-profile 0/1**
(config-count-prof 0/1)**#color green**

Technology Review

Color parameters represent bandwidth profiles. There are four basic profiles:

- CIR is the average rate up to which Service Frames are delivered. Service Frames are always sent at the User-to-Network (UNI) speed.
- Committed Burst Size (CBS) is the maximum number of bytes allowed for incoming Service Frames to still be CIR compliant.
- EIR is the average rate up to which excess Service Frames (frames whose average rate is greater than CIR) are admitted into the network.
- Excess Burst Size (EBS) is the maximum number of bytes allowed for incoming Service Frames to be EIR complaint.

A service frame is green if it is compliant with CIR/CBS of the bandwidth profile. A service frame is yellow if it is greater than the CIR/CBS of the profile, but less than the EIR/EBS. A service Frame is ‘Red’ if it is not compliant with either the CIR/CBS or EIR/EBS.

Green service frames are delivered per the performance objective and not generally discarded because they are in profile. Yellow service frames are out of profile, but are not typically discarded unless network conditions (for example, congestion) prevents delivery. Red service frames are out of profile and immediately discarded.

pbit <*number*>

Use the **pbit** command to include the virtual local area network (VLAN) priority bit in the matching criteria for the counter profile. Use the **no** form of this command to remove the VLAN priority bit from the matching critera.

Syntax Description

<*number*>	Specifies the value of the VLAN priority bit to be used for the matching criteria for the counter profile. Valid range is **0** to **7**.

Default Values

By default, the VLAN priority is not included in the matching criteria for counter profiles.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example adds VLAN priority **3** to the matching criteria for the counter profile:

(config)**#counter-profile 0/1**
(config-count-prof 0/1)**#pbit 3**

vlan

Use the **vlan** command to include the virtual local area network identifier (VLAN ID) to the matching criteria for the counter profile. Use the **no** form of this command to remove the VLAN ID from the matching criteria. Variations of this command include:

vlan <*vlan id*>
vlan none

Syntax Description

<*vlan id*>	Specifies the VLAN ID to include in the matching criteria for the counter profile. Valid range is **0** to **4094**.
none	Specifies that only untagged traffic is included in the matching criteria for the counter profile.

Default Values

By default, VLAN IDs are not included in the matching criteria for counter profiles.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example includes only untagged traffic in the matching criteria for the counter profile:

(config)**#counter-profile 0/1**
(config-count-prof 0/1)**#vlan none**

DESKTOP AUDITING LOCAL POLICY COMMAND SET

Desktop auditing is an AOS feature that uses Dynamic Host Configuration Protocol (DHCP) in conjunction with the Microsoft® Network Access Protection (NAP) Protocol to monitor the health of client computers connected to a NetVanta network. The two protocols work together to ensure that systems connected to the network are using appropriate corporate policies, such as appropriate firewall settings, antivirus settings, and other client health information. This information is exchanged between clients and servers in statement of health (SoH) and statement of health response (SoHR) messages.

Desktop auditing is configured on AOS products by enabling the feature and by optionally configuring filters to limit the output of the collected NAP information. These optional filters allow you to see who the policy violators are. When desktop auditing is enabled, the AOS product collects DHCP information, such as the medium access control (MAC) and IP addresses, virtual local area network (VLAN) ID, host name, and source port, as well as the MAC and IP addresses of the server and the date and time of the last DHCP information update. The NAP information collected by desktop auditing includes the client's OS version and service pack, processor architecture, firewall name and state, antivirus name and state, antispyware name and state, automatic update configuration, security update information, and the NAP state (enabled or disabled) of both the server and the client.

Desktop auditing local policies determine when a NAP client may be a violator by collecting NAP information for the connected clients and comparing them to the configured policies. It is possible to monitor clients' firewall states, antivirus states, antispyware states, auto-update states, and security update statuses using these policies. If no desktop auditing policies are configured, then, by default, desktop auditing monitors all NAP information for each client.

For more information about configuring desktop auditing, refer to the *Configuring Desktop Auditing in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Desktop auditing should be enabled on the AOS device before configuring the desktop auditing local policy. Desktop auditing is enabled using the command *desktop-auditing dhcp on page 1257*. To create a desktop auditing local policy and enter the policy's configuration mode, enter the **desktop-auditing local-policy** command from the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#desktop-auditing local-policy
(desktop-audit-policy)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

do on page 81
exit on page 83

All other commands in this command set are described in this section in alphabetical order:

anti-spyware current

Use the **anti-spyware current** command to define the local desktop auditing policy to monitor clients' antispyware status. If the antispyware is inactive, disabled, or not up-to-date, the client is a violator and its statistics will be collected. Using the **no** form of this command removes antispyware monitoring from the policy.

Syntax Description

No subcommands.

Default Values

By default, desktop monitoring local policies monitor all NAP information for each client.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following example specifies that the local policy will monitor clients' antispyware status:

(config)**#desktop-auditing local-policy**
(desktop-audit-policy)**#anti-spyware current**

anti-virus current

Use the **anti-virus current** command to define the local desktop auditing policy to monitor clients' antivirus status. If the antivirus is inactive, disabled, or not up-to-date, the client is a violator and its statistics will be collected. Using the **no** form of this command removes antivirus monitoring from the policy.

Syntax Description

No subcommands.

Default Values

By default, desktop monitoring local policies monitor all NAP information for each client.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following example specifies that the local policy will monitor clients' antivirus status:

(config)**#desktop-auditing local-policy**
(desktop-audit-policy)**#anti-virus current**

auto-update current

Use the **auto-update current** command to define the local desktop auditing policy to monitor clients' auto-update status. If the auto-updates are not configured to check for updates, download them, and install them automatically, then the client is a violator and its statistics will be collected. Using the **no** form of this command removes auto-update monitoring from the policy.

Syntax Description

No subcommands.

Default Values

By default, desktop monitoring local policies monitor all NAP information for each client.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following example specifies that the local policy will monitor clients' auto-update status:

(config)**#desktop-auditing local-policy**
(desktop-audit-policy)**#auto-update current**

firewall enable

Use the **firewall enable** command to define the local desktop auditing policy to monitor clients' firewall states. If the firewall is disabled or inactive, the client is a violator and its statistics will be collected. Using the **no** form of this command removes firewall monitoring from the policy.

Syntax Description

No subcommands.

Default Values

By default, desktop monitoring local policies monitor all NAP information for each client.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following example specifies that the local policy will monitor clients' firewall states:

(config)**#desktop-auditing local-policy**
(desktop-audit-policy)**#firewall enable**

security-update current

Use the **security-update current** command to define the local desktop auditing policy to monitor clients' security update status. If security updates are not current, the client is a violator and its statistics will be collected. Using the **no** form of this command removes security update monitoring from the policy.

Syntax Description

No subcommands.

Default Values

By default, desktop monitoring local policies monitor all NAP information for each client.

Command History

Release 17.8	Command was introduced.

Usage Examples

The following example specifies that the local policy will monitor clients' security update status:

(config)**#desktop-auditing local-policy**
(desktop-audit-policy)**#security-update current**

DYNAMIC COUNTER CONFIGURATION COMMAND SET

The Dynamic Counter Configuration Command Set allows you to create a dynamic counter. Dynamic counters are used to monitor traffic as it is transmitted to, or received from any interface. After a dynamic counter is created, it is assigned an interface to monitor and a counter profile that defines the matching criteria for traffic to monitor on the interface. For example, the counter profile can be configured to monitor any green traffic being received on a particular VLAN from a specified EFM bonding group, or it can be configured to monitor red traffic on a particular VLAN being discarded by the policer.

Dynamic counters are created and configured using the dynamic-counter command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#dynamic-counter 0/1
(config-dyn-count 0/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

set counter-profile <slot/index> on page 4403
set interface <interface> on page 4404

set counter-profile <*slot/index*>

Use the **set counter-profile** command to assign a specific counter profile to the dynamic counter. The counter profile is used to specify additional matching criteria for counting packets on the interface. Use the **no** form of this command to remove counter profile from the dynamic counter. Variations of this command include:

set counter-profile <*slot/index*> **exclude**
set counter-profile <*slot/index*> **include**

Syntax Description

<*slot/index*>	Specifies the index of the counter profile to assign to the dynamic counter in the format <*slot/index*>.
exclude	Specifies that the dynamic counter will count packets that do not match the counter profile.
include	Specifies that the dynamic counter will count packets that match the counter profile.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

A counter profile provides additional filtering capabilities to dynamic counters. Only one counter profile can be attached to each dynamic counter; however, a single counter profile can be attached to more than one dynamic counter.

Usage Examples

The following example specifies that the dynamic counter will count packets on the interface that match the criteria specified in counter profile **0/1**:

(config)**#dynamic-counter 0/1**
(config-dyn-count 0/1)**#set counter-profile 0/1 include**

set interface <*interface*>

Use the **set interface** command to specify an interface to be monitored by the dynamic counter. Use the **no** form of this command to remove the dynamic counter from the interface. Variations of this command include:

set interface <*interface*> **queue** <*queue*> **[congestion-drop | dqueue | enqueue]**
set interface <*interface*> **rx**
set interface <*interface*> **tx**

Syntax Description

<*interface*>	Specify an interface to be monitored by the dynamic counter in the format <*interface type [slot/port	slot/port.subinterface id	interface id	interface id.subinterface id	ap	ap/radio	ap/radio.vap]*>. For example, for a Gigabit Ethernet interface, use **gigabit-ethernet 0/1**; for an EFM group, use **efm-group 0/1**.
queue <*queue*>	Specifies that queue statistics for the specified queue will be collected by the dynamic counter. Valid range is **0** to **n**.
congestion-drop	Specifies that packets chosen by the congestion manager to be dropped rather than enqueued are counted.
dequeued	Specifies that packets that have successfully left the queue to be sent on the interface are counted.
enqueued	Specifes that packets that have entered the queue are counted.
rx	Specifies that packets recieved by the specified interface are counted.
dx	Specifies that packets transmitted by the specified interface are counted.

Default Values

No default values are necessary for this command.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example specifies that the dynamic counter will count packets received by Gigabit Ethernet interface **0/1**:

(config)**#dynamic-counter 0/1**
(config-dyn-count 0/1)**#set interface gigabit-ethernet 0/1 rx**

ETHERNET OAM CFM COMMAND SET

Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) is a type of service management for wide area network (WAN) Ethernet networks over an entire Ethernet service instance. Ethernet OAM CFM provides maintenance and monitoring within multiple network domains and different domain levels, and is specifically concerned with detecting faults over the service instance. Using a system of messages and notifications within the service domain, CFM can discover Ethernet service instance connection paths, locate and verify faults in the connection, isolate any discovered faults, give notification of discovered faults, and assist in fault recovery.

CFM operates between maintenance domains (MDs), MD levels, maintenance intermediate points (MIPs), and maintenance endpoints (MEPs). MDs are administrator domains of switches and routers, created for the purpose of managing a WAN network. Each MD is nested in a hierarchy, and these hierarchies create MD levels. Each level is specific to the MD, as each level is made up of a different MD along the service instance. These levels are created by the beginning and termination of MDs using MIPs and MEPs. MIPs are maintenance points within the MD, and MEPs are maintenance points that terminate the domain.

Ethernet OAM CFM in AOS deals specifically with MEPs in the AOS product. MEPs terminate Layer 2 traffic and are typically routers that convert Layer 2 traffic into a Layer 3 interface. CFM detects service connectivity problems by sending continuity check messages (CCMs) between MEPs, by sending path trace messages (Ethernet traceroute) between MEPs, and by sending loopback messages (Ethernet ping) between MEPs.

The Ethernet OAM CFM command set describes the commands needed for configuring MDs, maintenance associations (MAs), and MEPs. To enable Ethernet OAM CFM functionality, enter the command *ethernet cfm on page 1273* from the Global Configuration mode prompt as follows:

```
>enable
#configure terminal
(config)#ethernet cfm
(config)#
```

Once Ethernet OAM CFM is enabled, you must create a maintenance domain using the **ethernet cfm domain** <*name*> **level** <*level*> command (refer to *ethernet cfm domain on page 1274*). This command is entered from the Global Configuration mode prompt, and enters the maintenance domain configuration. Enter the command as follows:

```
>enable
#configure terminal
(config)#ethernet cfm domain domain1 level 6
(config-ecfm-domain)#
```

After entering the MD Configuration mode, you can access the MA Configuration mode, the MEP Configuration mode, and the Interface Configuration mode. The following command set describes commands common to all CFM Configuration modes, as well as those specific to maintenance association (MA), MEP, or Interface configurations. For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83
interface on page 84

The following commands are MD configuration commands:

association <name> on page 4407
remote-mep hold-time <minutes> on page 4408

The **association** <*name*> command, as described in the MD configuration command section, creates an MA and enters the MA Configuration mode. The following commands are MA configuration commands:

ccm interval on page 4409
component <component> vlan on page 4410
mep-validation on page 4412
remote-mep <mep id> on page 4414

The **component** command, as described in the MA configuration command section, creates a component and enters the Component Configuration mode. The following commands are component configuration commands:

mp-sender-id on page 4415

Ethernet OAM CFM can also be configured at the interface level. CFM must be enabled and an MEP must be created at the interface level using the commands *ethernet-cfm down on page 2174* and *ethernet-cfm mep on page 2175* from the Ethernet or Ethernet subinterfaces. Once CFM is enabled and the MEP is created at the interface level, the MEP can be configured using the following commands:

alarm-priority-level on page 4416
alarm timers <alarm time> <reset time> on page 4418
ccm-enabled on page 4419
mep-enabled on page 4420
priority <value> on page 4421
snmp-trap fault alarm on page 4422

association *<name>*

Use the **association** command to create, enable, and enter the configuration of an Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) maintenance association (MA). Use the **no** form of this command to remove the association and its association maintenance endpoints (MEPs).

Syntax Description

<name>	Specifies the name of the MA. Names can be up to 42 characters in length.

Default Values

By default, no MAs exist.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables and creates MA **association1** from the Maintenance Domain (MD) Configuration mode, and enters the MA Configuration mode:

```
(config)#ethernet cfm domain domain1 level 6
(config-ecfm-domain)#association association1
(config-ecfm-assoc)#
```

remote-mep hold-time <*minutes*>

Use the **remote-mep hold-time** command to specify the length of time an associated maintenance endpoint (MEP) remains in the maintenance domain's (MD's) remote MEP database after the MEP has entered a failed state. Use the **no** form of this command to return to the default value.

Syntax Description

<*minutes*>	Specifies the length of time the associated MEP remains in the MD's MEP database after the MEP has failed. Range is **1** to **65535** minutes.

Default Values

By default, MEPs remain in the MD's MEP database for **100** minutes.

Command History

Release 17.4	Command was introduced.

Functional Notes

Each MEP that is created is associated with a particular MD. The MDs maintain an MEP database of remote MEPs, listing all configured and associated remote MEPs within the system. When a remote MEP fails, it can be removed from this database after a specified amount of time. When the remote MEP entry is purged, any errors logged relating to the remote MEP are also purged.

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that remote MEP entries are purged from the MD's remote MEP database after **60** minutes:

```
(config)#ethernet cfm domain domain1 level 6
(config-ecfm-domain)#remote-mep hold-time 60
(config-ecfm-domain)#
```


ccm interval

Use the **ccm interval** command to specify how frequently maintenance endpoints (MEPs) of this association send continuity check messages (CCMs). Use the **no** form of this command to return to the default value. Variations of this command include:

ccm interval 100ms
ccm interval 1s
ccm interval 10s
ccm interval 1m
ccm interval 10m

Syntax Description

100ms	Specifies the interval as 100 milliseconds.
1s	Specifies the interval as 1 second.
10s	Specifies the interval as 10 seconds.
1m	Specifies the interval as 1 minute.
10m	Specifies the interval as 10 minutes.

Default Values

By default, the continuity check message (CCM) interval is set to **1** second.

Command History

Release 17.4	Command was introduced.

Functional Notes

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example sets the CCM interval to **1** minute:

```
(config-ecfm-domain)#association association1
(config-ecfm-assoc)#ccm interval 1m
(config-ecfm-assoc)#
```

component <*component*> vlan

Use the **component vlan** command to create a set of virtual local area networks (VLANs) as a fixed group on a particular component and assign these VLANs to be protected by the maintenance association (MA) on this component. The command also enters the Component Configuration mode. The **no** form of this command removes the component definition from the association. Variations of this command include:

component <*component*> **vlan none**
component <*component*> **vlan** <*vlan id*>

Syntax Description

<*component*>	Specifies the component to be added to the MA. Components are specified in the form <*component type [slot/port]*>. For example, for an Ethernet component, use **eth 0/1**. To discover available components, enter **component ?** at the prompt.
vlan none	Specifies that this MA component is not attached to a virtual local area network (VLAN).
vlan <*vlan id*>	Specifies to which VLAN this MA component is attached. VLAN IDs range from **1** to **4094**.

Default Values

By default, no component is defined.

Command History

Release 17.4	Command was introduced.
Release A5.01	Command was expanded to include the Gigabit Ethernet component.

Functional Notes

At least one component must be added to each MA. The components and VLANs are associated so that the VLANs are protected by the MA to which the component belongs. The first VLAN ID listed is the primary VLAN ID for the entry being created.

A component must be configured on a VLAN before you can configure its associated maintenance endpoint (MEP).

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example configures an **Ethernet** component that is associated with **vlan 5**, and enters the Component Configuration mode:

(config-ecfm-domain)**#association association1**
(config-ecfm-assoc)**#component ethernet 0/1 vlan 5**
(config-ecfm-ma-comp)#

mep-validation

Use the **mep-validation** command to specify whether or not maintenance endpoints (MEPs) use a comparison between their continuity check message (CCM) database (received CCMs) and their list of configured remote MEPs (that should be sending CCMs) to generate an alarm when a mismatch is discovered. The **no** form of this command disables MEP validation. Variations of this command include:

mep-validation
mep-validation start-delay *<delay>*

Syntax Description

start-delay *<delay>*	Optional. Specifies a delay (in seconds) that the MEP will wait before enforcing MEP validation. Delay range is **1** to **65535** seconds.

Default Values

By default, MEP validation is enabled with a delay of **30** seconds.

Command History

Release 17.4	Command was introduced.

Functional Notes

The MEP validation is used to compare an MEP's list of received CCMs with a list of MEPs that should be sending CCMs. When MEP validation is enabled, an alarm is sent when a mismatch is discovered. By default, each MEP validates their MEP list, and all CCMs received must correspond to preconfigured remote MEPs in the maintenance association (MA).

Disabling validation (using the **no** form of the command), or changing the start delay, can be useful when creating a domain association or when troubleshooting. Disabling validation in these circumstances prevents unnecessary alarms and warnings. For example, if you wish to allow the unit to dynamically learn its remote MEPs rather than manually entering them, disabling validation allows you to do that without generating unnecessary alarms.

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example disables MEP validation:

(config-ecfm-domain)**#association association1**
(config-ecfm-assoc)**#no mep-validation**
(config-ecfm-assoc)#

The following example changes the delay interval to **1000** seconds:

(config-ecfm-domain)**#association association1**
(config-ecfm-assoc)**#mep-validation start-delay 1000**
(config-ecfm-assoc)#

remote-mep *<mep id>*

Use the **remote-mep** command to create a list of remote maintenance endpoints (MEPs) for this association. Use the **no** form of this command to remove the MEP from the list.

Syntax Description

<mep id>	Specifies the unique ID given to the MEP. MEP ID range is **1** to **8191**.

Default Values

By default, no remote MEPs are listed.

Command History

Release 17.4	Command was introduced.

Functional Notes

Using the **remote-mep** command populates the maintenance association's (MA's) remote MEP list. Remote MEPs are MEPs not on this device, but communicate with other MEPs in the same MA. Local MEPs, or those on the same device, are automatically listed.

Each MEP ID is stored and can be compared to the MEP's continuity check message (CCM) database learned by listening to CCMs from other MEPs in the network. This allows each MEP to determine if it is receiving CCMs from expected MEPs, as well as detect any unexpected MEPs in the network.

You will need to repeat this command as many times as necessary to populate the MA's remote MEP list with all of the remote MEPs in your network.

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example adds the remote MEP with the MEP ID of **1000** to this association's remote MEP list:

```
(config-ecfm-domain)#association association1
(config-ecfm-assoc)#remote-mep 1000
(config-ecfm-assoc)#
```

mp-sender-id

Use the **mp-sender-id** command to enable each maintenance endpoint (MEP) in this association to send sender ID type length values (TLVs) in transmitted packets. Use the **no** form of this command to revert the sender ID setting to that of the parent association. Variations of this command include:

mp-sender-id chassis-id
mp-sender-id chassis-id management-address
mp-sender-id management-address
mp-sender-id management-address chassis-id
mp-sender-id none

Syntax Description

chassis-id	Specifies that the chassis IDs are transmitted.
management-address	Specifies that management addresses are transmitted.
none	Specifies that no sender ID is transmitted.

Default Values

By default, the MEP's sender ID setting is the same as that of the parent association.

Command History

Release 17.4	Command was introduced.

Functional Notes

TLVs are included in continuity check messages (CCMs) and used in Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) fault detection.

It is important to note how the **chassis ID** and **management address** are created for the system. The chassis ID is created either from Simple Network Management Protocol (SNMP), using the command *snmp-server chassis-id "<string>" on page 1786*, or if SNMP is not configured, using the system medium access control (MAC) address. The management address is created either from SNMP through the primary IP of the source interface shown in the command *snmp-server source-interface <interface> on page 1819*, or if SNMP is not configured, using the primary IP of the MEP's interface.

For more information regarding Ethernet OAM CFM and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that MEPs in this association include their **chassis ID** in the sender ID TLVs:

```
(config-ecfm-domain)#association association1
(config-ecfm-ma-comp)#mp-sender-id chassis-id
(config-ecfm-ma-comp)#
```

alarm-priority-level

Use the **alarm-priority-level** command to configure the lowest level priority condition that generates an alarm on this maintenance endpoint (MEP). Use the **no** form of this command to return to the default priority condition. Variations of this command include:

alarm-priority-level errorccm
alarm-priority-level macstatus
alarm-priority-level none
alarm-priority-level rdi-ccm
alarm-priority-level remoteccm
alarm-priority-level xconccm

Syntax Description

errorccm	Specifies that priority conditions of **4** or higher generate alarms.
macstatus	Specifies that priority conditions of **2** or higher generate alarms.
none	Specifies that no priority conditions generate alarms.
rdi-ccm	Specifies that priority conditions of **1** or higher generate alarms.
remoteccm	Specifies that priority conditions of **3** or higher generate alarms.
xconccm	Specifies that priority conditions of **5** or higher generate alarms.

Default Values

By default, priority conditions of **1** or higher generate alarms.

Command History

Release 17.4	Command was introduced.

Functional Notes

Alarm notifications are sent either by using the AOS event priority system or through Simple Network Management Protocol (SNMP) notification. The alarms are sent as priority 1 (error), and cleared alarms are sent as priority 3 (notice). SNMP notification of alarms are sent to the fault alarm address configured on the MEP reporting the fault. No SNMP notification is sent when an alarm clears. You can specify using SNMP notification for alarms by using the command *snmp-trap fault alarm on page 4422*.

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

The following table describes the five Ethernet OAM CFM defect conditions, as well as the root cause, the priority, and the importance of each.

Defect	Description	Cause(s)	Priority	Importance
DefXconCCM	Indicates an MEP that could be from another MA is sending CCMs to an MEP in this MA.	The CCM received is from an MEP that does not have a MAID that matches the local MEP's MAID, or that the transmitting MEP has an MD level lower than the local MEP's.	5	Highest
DefErrorCCM	Indicates erroneous CCMs are being received from some MEP in the local MEP's MA.	The transmitting MEP's ID is not in the MA's configured list of remote MEPs, the MEP ID is not the same as the receiving MEP's ID, or the CCM interval does not match the configured value.	4	
DefRemoteCCM	Indicates the local MEP is not receiving CCMs from an MEP in its configured list.	An MEP in this MEP's configured list has not sent a CCM in three CCM intervals.	3	
DefMACStatus	Indicates the last CCM received by this MEP from another MEP indicated the other MEP's associated MAC is reporting an error status via the Port or Interface Status TLV.	Either all remote MEPs are reporting Port Status TLV errors, or at least one remote MEP is reporting an Interface Status TLV error.	2	
DefRDICCM	Indicates the last CCM received by this MEP from some remote MEP contained the remote defect indication (RDI) bit.	At least one MEP is reporting RDI.	1	Lowest

Usage Examples

The following example specifies that events of a priority **3** or higher generate alarms:

(config-eth 0/1)**#ethernet-cfm mep Domain1 association1 100 down**
(config-eth 0/1-mep)**#alarm-priority-level remoteccm**
(config-eth 0/1-mep)#

alarm timers *<alarm time> <reset time>*

Use the **alarm timers** command to specify the amount of time a defect condition must occur in the maintenance endpoint (MEP) before it triggers an alarm and how long a defect condition must be absent before a new alarm can be triggered. Use the **no** form of this command to set the timers to their default value.

Syntax Description

<alarm time>	Specifies the time that a defect condition must be present before it is eligible to be reported as an alarm. Range is **2500** to **10000** milliseconds.
<reset time>	Specifies the time that defects must be absent before alarms are reset such that a new alarm can be triggered. Range is **2500** to **10000** milliseconds.

Default Values

By default, the alarm time is **2500** ms and the reset time is **10000** ms.

Command History

Release 17.4	Command was introduced.

Functional Notes

Timer values are stored in 1/1000 of a second. Therefore, entering the command as follows:

alarm timers 2514 10239

stores the timer values as **2510** and **10230**.

Defect conditions are the problems detected by Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM). These conditions are detailed in the *Functional Notes* section of the **alarm-priority-level** command. For more information on defect conditions and Ethernet OAM CFM in general, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the alarm time is **3000** ms and the reset time is **6000** ms for this MEP's alarm timers:

```
(config-eth 0/1)#ethernet-cfm mep Domain1 association1 100 down
(config-eth 0/1-mep)#alarm timers 3000 6000
(config-eth 0/1-mep)#
```

ccm-enabled

Use the **ccm-enabled** command to enable maintenance endpoint (MEP) continuity check message (CCM) transmissions. Use the **no** form of this command to disable CCM transmissions on the MEP.

Syntax Description

No subcommands.

Default Values

By default, CCM transmissions are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

Even when CCM transmissions are disabled, the MEP can still process received CCMs.

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) and its operation on AOS products, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables CCM transmissions on the MEP:

```
(config-eth 0/1)#ethernet-cfm mep Domain1 association1 100 down
(config-eth 0/1-mep)#ccm-enabled
(config-eth 0/1-mep)#
```

mep-enabled

Use the **mep-enabled** command to enable the maintenance endpoint (MEP) and all the MEPs in its association. Use the **no** form of this command to halt all associated MEP functionality for this MEP.

Syntax Description

No subcommands.

Default Values

By default, all MEPs are disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

When an MEP is disabled, no frames are sent or received by the MEP, but all other configuration properties are retained.

For more information regarding Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM), refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables an MEP:

```
(config-eth 0/1)#ethernet-cfm mep Domain1 association1 100 down
(config-eth 0/1-mep)#mep-enabled
(config-eth 0/1-mep)#
```

priority *<value>*

Use the **priority** command to specify the 802.1p priority given to Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) frames and linktrace messages transmitted by the maintenance endpoint (MEP). Use the **no** form of this command to return the priority to the default value.

Syntax Description

<value>	Specifies the priority. Range is **0** to **7**.

Default Values

By default, the priority value is **7**.

Command History

Release 17.4	Command was introduced.

Functional Notes

Priority only applies to CFM frames if the MEP's interface supports virtual local area network (VLAN) tags and the message will be sent with a tag.

For more information regarding Ethernet OAM CFM, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies a priority of **3** for CFM frames and linktrace messages transmitted by this MEP:

```
(config-eth 0/1)#ethernet-cfm mep Domain1 association1 100 down
(config-eth 0/1-mep)#priority 3
(config-eth 0/1-mep)#
```

snmp-trap fault alarm

Use the **snmp-trap fault alarm** command to configure and send Simple Network Management Protocol (SNMP) traps for fault alarms generated from a maintenance endpoint (MEP). Use the **no** form of this command to disable SNMP fault alarm notification.

Syntax Description

No subcommands.

Default Values

By default, SNMP fault alarm notification is disabled.

Command History

Release 17.4	Command was introduced.

Functional Notes

SNMP notification is an alternate method to configuring and receiving Ethernet operations, administration, and maintenance (OAM) connectivity fault management (CFM) alarm notifications through the AOS event priority system. SNMP notifications of alarms are sent to the fault alarm address configured on the MEP reporting the fault. No SNMP notification is sent when an alarm clears.

For more information regarding Ethernet OAM CFM, refer to the *Ethernet OAM CFM in AOS* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables SNMP notification for alarm notifications from this MEP:

```
(config-eth 0/1)#ethernet-cfm mep Domain1 association1 100 down
(config-eth 0/1-mep)#snmp-trap fault alarm
(config-eth 0/1-mep)#
```

MAIL AGENT COMMAND SET

The mail agent feature of Adtran Operating System (AOS) provides a method of adding email notification to any AOS feature. The mail agent is configured through the command line interface (CLI) and operates with any AOS feature that has configuration or **show** commands. The mail agent captures output from specified commands and emails them to a specified address in the body of an email message. Email messages are created when a specified event occurs, and are mailed on a specified schedule. Multiple mail agents can be configured and used at one time. For more information about the creation of mail agents and their capabilities, refer to the *Generic Mail Agent quick configuration guide* available online at https://supportcommunity.adtran.com.

To activate the Mail Agent Configuration mode, enter the **mail-client** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#mail-client myagent
(config-mail-client-myagent)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

address on page 4424
body size <bytes> on page 4425
capture commands on page 4426
capture header on page 4427
capture trigger on page 4428
send test on page 4430
send trigger on page 4431
server <dns-name/ip address> on page 4432
subject <text> on page 4433

address

Use the **address** command to specify the CC, From, and To fields in the email messages. Use the **no** form of this command to remove the specified information from the email header. Variations of this command include:

address cc *<email address(es)>*
address from *<email address(es)>*
address to *<email address>*

Syntax Description

cc *<email address(es)>*	Specifies the CC field in the email message. Multiple email addresses are separated by semicolons.
from *<email address(es)>*	Specifies the From field in the email message. Multiple email addresses are separated by semicolons.
to *<email address>*	Specifies the To field in the email message.

Default Values

By default, the CC value is empty. The To default value is set using the command *logging email address-list <email address> ; <email address> on page 1582* and the From default value is set using the command *logging email sender on page 1594*.

Command History

Release 17.2	Command was introduced.

Functional Notes

The **address to** command uses a default value from the command *logging email address-list <email address> ; <email address> on page 1582*. If the **logging email address-list** command has been configured, and the mail agent notification will go to the same email, using the **address to** command is not necessary.

Usage Examples

The following example configures the CC, From, and To fields in the email notification sent by mail agent **myagent**:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#address to manager@company.net**
(config-mail-client-myagent)**#address cc fellowemployee@company.net; assistntmngr@company.net**
(config-mail-client-myagent)**#address from goodemployee@company.net**

body size <*bytes*>

Use the **body size** command to set the maximum buffer size for the body text of the email message. Use the **no** form of this command to return to the default value.

Syntax Description

<*bytes*>	Specifies the maximum number of bytes the buffer holds. Range is **1** to **65535** bytes.

Default Values

By default, the buffer size is set to **4048** bytes.

Command History

Release 17.2	Command was introduced.

Functional Notes

All output generated after the buffer size has been reached will be ignored.

Usage Examples

The following example sets the body text buffer size to **6000** bytes for mail agent **myagent**:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#body size 6000**

capture commands

Use the **capture commands** command to specify the command output to capture and include in the body of the email. Use the **no** form of this command to remove the specified commands.

Syntax Description

No subcommands.

Default Values

By default, no commands are specified.

Command History

Release 17.2	Command was introduced.

Functional Notes

The **capture commands** command specifies the command output to be captured by the mail agent. **Show** and **tcl** commands can be captured. When the **capture commands** command is entered, each command to be captured is specified with the **do** keyword followed by the command. The terminal configuration mode is enabled by default for the **capture commands** command, making it necessary to use the keyword **do**. List all commands to be sent in a single notification, followed by the **exit** keyword.

Usage Examples

The following example specifies that the mail agent **myagent** will capture the output from the **show ip route** and **show clock** commands:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#capture commands**
Enter the commands you wish to run, one line at a time.
Entries are run from the terminal configuration prompt.
For example, you must enter ‘do show run’ or ‘int eth 0/1’.
When finished, type ‘exit’ on a new line to end.
#do show ip route
#do show clock
#exit
(config-mail-client-myagent)#

capture header

Use the **capture header** command to specify that header information (ASCII demarcation and a timestamp) is included when command output is captured. Use the **no** form of this command to remove the header information from captured command output.

Syntax Description

No subcommands.

Default Values

By default, header information is included in captured command output.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example removes header information from the captured command output for mail agent **myagent**:

```
(config)#mail-client myagent
(config-mail-client-myagent)#no capture header
```

capture trigger

Use the **capture trigger** command to configure the trigger that causes the mail agent to capture the command output. Use the **no** form of this command to remove the trigger. Variations of this command include:

capture trigger
capture trigger track <*name*> **fail**
capture trigger track <*name*> **pass**

Syntax Description

track <*name*> **fail**	Optional. Specifies the command output is captured when the named track changes from a pass state to a fail state.
track <*name*> **pass**	Optional. Specifies the command output is captured when the named track changes from a fail state to a pass state.

Default Values

By default, no tracks are configured and no trigger is defined.

Command History

Release 17.2	Command was introduced.

Functional Notes

If no trigger is specified, the mail agent will immediately run the specified commands and capture their output. If a track is specified as the capture trigger, the command output will be captured every time the track switches to the specified state. The track used should be a preconfigured track with an associated schedule. The track will change states when its associated schedule becomes active or inactive. For more information on schedules, refer to *schedule <name> on page 1695*. For more information on tracks, refer to the *Network Monitor Track Command Set on page 4098* of this guide. For more information on the functions of tracks and schedules as part of the mail agent feature, refer to the *Generic Mail Agent quick configuration guide* available online at https://supportcommunity.adtran.com.

The command *send trigger on page 4431* can be used without the **capture trigger** command. If only the **send trigger** command is used, the **send trigger** command will function as the **capture trigger** command and immediately capture the command output and send an email of the captured output. If both commands are used, the command output is captured at the time the capture trigger occurs, and then an email is sent at the time the send trigger occurs.

Usage Examples

The following example specifies that when the track **mail** changes to a **pass** state, the mail agent **myagent** will capture command output:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#capture trigger track mail pass**

send test

Use the **send test** command to have the mail agent send a test email message to the email address(es) specified by the **address to** command (refer to *address on page 4424*) or the **logging email address-list** command (refer to *logging email address-list <email address> ; <email address> on page 1582*).

Syntax Description

No subcommands.

Default Values

By default, the test email is sent using your Simple Mail Transfer Protocol (SMTP) settings even if the mail client is currently shut down.

Command History

Release 17.2	Command was introduced.

Functional Notes

The command appends “This is a test message” onto the current message buffer and sends an email to the configured addresses. This command is used to test that the agent is sending emails to the proper addresses.

Usage Examples

The following example instructs mail agent **myagent** to send a test email to the previously configured email addresses:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#send test**

send trigger

Use the **send trigger** command to configure when an email with command output is sent to the email address(es) specified by the **address to** command (refer to *address on page 4424*) or the **logging email address-list** command (refer to *logging email address-list <email address> ; <email address> on page 1582*). Use the **no** form of this command to remove the configuration. Variations of this command include:

send trigger
send trigger track <*name*> **fail**
send trigger track <*name*> **pass**

Syntax Description

track <*name*> **fail**	Optional. Specifies the email message is sent when the named track changes from a pass state to a fail state.
track <*name*> **pass**	Optional. Specifies the email message is sent when the named track changes from a fail state to a pass state.

Default Values

By default, no email is sent.

Command History

Release 17.2	Command was introduced.

Functional Notes

If no trigger is specified, the mail agent will immediately send the email. If a track is specified as the send trigger, the email will be sent every time the track switches to the specified state. The track used should be a preconfigured track with an associated schedule. The track will change states when its associated schedule becomes active or inactive. For more information on schedules, refer to the command *schedule <name> on page 1695*. For more information on tracks, refer to the *Network Monitor Track Command Set on page 4098* of this guide. For more information on the functions of tracks and schedules as part of the mail agent feature, refer to the *Generic Mail Agent quick configuration guide* available online at https://supportcommunity.adtran.com.

The **send trigger** command can be used without the **capture trigger** command (refer to *capture trigger on page 4428*). If only the **send trigger** command is used, the **send trigger** command will function as the **capture trigger** command and immediately capture the command output and send an email of the captured output. If both commands are used, the command output is captured at the time the capture trigger occurs, and then an email is sent at the time the send trigger occurs.

Usage Examples

The following example specifies when the track named **sendmail** changes to a **fail** state, mail agent **myagent** will send an email with captured command output:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#send trigger track sendmail fail**

server *<dns-name/ip address>*

Use the **server** command to specify the Simple Mail Transfer Protocol (SMTP) server for sending mail agent notifications. Use the **no** form of this command to return the server setup to the default value.

Syntax Description

<dns-name>	Specifies the domain naming system (DNS) name of the SMTP server.
<ip address>	Specifies the IP address of the SMTP server. IP addresses are expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, the SMTP server is set to the value defined by the command *logging email receiver-ip <ipv4 address | hostname> on page 1591*.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example specifies that mail agent **myagent** use the SMTP server at IP address **172.5.67.99** to send email messages:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#server 172.5.67.99**

subject <*text*>

Use the **subject** command to specify the Subject field in the mail agent email message. Use the **no** form of this command to clear the Subject field.

Syntax Description

<*text*>	Specifies the text of the Subject field.

Default Values

By default, this field is empty.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example specifies a Subject of **report1** for the email message sent my mail agent **myagent**:

(config)**#mail-client myagent**
(config-mail-client-myagent)**#subject report1**

NETWORK SYNC COMMAND SET

Network synchronization (Network Sync) is a networking feature that provides clock synchronization at the physical network layer through Ethernet and Digital Subscriber Line (DSL) ports. The feature synchronizes clock frequency on a port by timing the interface's bit clock from clock signals received over the physical layer of the network. By using the physical layer, rather than an external time division multiplexed (TDM) circuit, remote network elements can receive reliable timing information through the packet network.

Network Sync uses messages through the Ethernet Synchronization Message Channel (ESMC) to provide clock information to remote network elements. The ESMC funnels synchronization status messages (SSMs) that indicate the quality level of a synchronization signal. Synchronization information is transmitted to the network elements through an egress clock, and the ESMC communications provide timing from the most reliable sources. Configuration of Network Sync in AOS depends upon, at a minimum, configuring a connection from which synchronization signals are recovered and a connection to which synchronization information is transmitted.

To access the Network Sync Configuration mode, enter the **network-sync** command from the Global Configuration mode as follows:

```
#configure terminal
(config)#network-sync
(config-ntwk-sync)#
```

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

connect on page 4435
eec-option on page 4437
esmc-process on page 4438
holdover threshold eec on page 4439
revertive priority on page 4440
ssm-override <input> on page 4441
transmit-ql-threshold <input> on page 4443
wait-to-restore <value> on page 4445

connect

Use the **connect** command to specify the interfaces from which clock information is recovered and to which clock information is transmitted. Clock information is typically recovered from network-to-network interfaces (NNIs) and typically transmitted to user-to-network interfaces (UNIs). Use the **no** form of this command to remove the interface from the network synchronization (Network Sync) configuration. Variations of this command include:

connect <*interface*> **recover primary**
connect <*interface*> **recover primary ssm**
connect <*interface*> **recover primary no-ssm**
connect <*interface*> **recover secondary**
connect <*interface*> **recover secondary ssm**
connect <*interface*> **recover secondary no-ssm**
connect <*interface*> **transmit**
connect <*interface*> **transmit ssm**
connect <*interface*> **transmit no-ssm**

Syntax Description

<*interface*>	Specifies the interface from which clock information is recovered, and to which clock information is sent. Specify interfaces in the format **interface type** <*slot/port*>. Available interfaces for Network Sync configuration are Gigabit Ethernet, single-pair high-speed digital subscriber line (SHDSL), and very high-speed digital subscriber line (VDSL) interfaces.
recover	Specifies that the interface is one from which clock information is recovered.
primary	Specifies the interface is the primary source for clock information.
secondary	Specifies the interface is the secondary source for clock information.
transmit	Specifies that the interface is one to which clock information is transmitted.
ssm	Optional. Specifies that SSMs are received on source interfaces and transmitted on receiving interfaces.
no-ssm	Optional. Specifies that SSMs are not received on source interfaces and are not transmitted on receiving interfaces.

Default Values

By default, no interfaces are specified for use with Network Sync. When interfaces are configured for Network Sync, SSM is enabled by default.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

For Network Sync to function, you must configure at least one interface as a clock source and one interface to which clock information is sent.

Usage Examples

The following example adds an interface to the Network Sync configuration as a primary clock source:

(config)**#network-sync**
(config-ntwk-sync)**#connect gigabit-ethernet 0/1 recover primary**

The following example specifies that Network Sync clock information is sent to the interface:

(config)**#network-sync**
(config-ntwk-sync)**#connect gigabit-ethernet 0/2 transmit**

eec-option

Use the **eec-option** command to specify which Ethernet equipment clock (EEC) option network synchronization (Network Sync) uses. Depending on the EEC option selected, available synchronization status message (SSM) override settings will differ (refer to the command *ssm-override <input> on page 4441*). Use the **no** form of this command to return to the default EEC option. Variations of this command include:

eec-option option1
eec-option option2

Syntax Description

option1	Specifies that EEC option 1 is used. This option is typically used in European networks.
option2	Specifies that EEC option 2 is used. This option is typically used in networks in the United States.

Default Values

By default, Network Sync uses EEC **option2**.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example changes the Network Sync EEC option:

(config)**#network-sync**
(config-ntwk-sync)**#eec-option option1**

esmc-process

Use the **esmc-process** command to enable Ethernet Synchronization Message Channel (ESMC) processing for network synchronization (Network Sync). ESMC processing provides a method for selecting the highest quality synchronization signal for remote network elements. Use the **no** form of this command to disable ESMC processing.

Syntax Description

No subcommands.

Default Values

By default, ESMC processing is disabled.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example enables Network Sync ESMC processing:

(config)**#network-sync**
(config-ntwk-sync)**#esmc-process**

holdover threshold eec

Use the **holdover threshold eec** command to enable the threshold for network synchronization (Network Sync) holdover mode. Use the **no** form of this command to remove the holdover threshold.

Syntax Description

No subcommands.

Default Values

By default, no holdover threshold is set. When the threshold is enabled, holdover is activated when the clock source quality is not greater than QL-EEC2.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

This command is used when the Ethernet Synchronization Message Channel (ESMC) process is active and when a recovered clock source is configured to receive synchronization status messages (SSMs). It affects operation when the received quality level is equal to that of an EEC. This is either QL-EEC1 or QL-EEC2, depending on whether EEC option 1 or EEC option 2 has been selected (refer to the command *eec-option on page 4437*). By default, a source is considered DOWN when its received quality level is at EEC. In this scenario, if there is a need for the source to stay UP, enter the **holdover threshold eec** command.

Below EEC, a source is always DOWN. Also, it is DOWN if the physical characteristics of its recovered clock are out of tolerance. When a source is DOWN, it is excluded from the network synchronization selection process. When all sources are DOWN, the unit goes into holdover mode.

Usage Examples

The following example keeps the source in an UP state:

(config)**#network-sync**
(config-ntwk-sync)**#holdover threshold eec**

revertive priority

Use the **revertive priority** command to specify that the network synchronization (Network Sync) clock selection is revertive based on clock priority. Use the **no** command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is enabled.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

Revertive clock selection means that if a clock source with a higher quality clock recovers after going down, Network Sync transitions back to the higher quality clock source as opposed to remaining on the currently selected clock source.

Usage Examples

The following example disables the revertive clock selection:

(config)**#network-sync**
(config-ntwk-sync)**#no revertive priority**

ssm-override *<input>*

Use the **ssm-override** command to configure the synchronization status message (SSM) override settings for network synchronization (Network Sync). Use the **no** form of this command to remove the override.

Syntax Description

<input>	Specifies the SSM quality level override option. Refer to the Functional Notes of this command for specifics.

Default Values

By default, SSM override options are those provided by Ethernet equipment clock (EEC) option 2.

Command History

Release R10.11.0	Command was introduced.

Functional Notes

The various *<input>* parameters available for SSM override vary according to the EEC option selected in the Network Sync configuration (refer to the command *eec-option on page 4437*). If you have not specified an EEC option, option 2 is used by default. The following tables outline the *<input>* parameters for the **ssm-override** command.

Table 3. SSM Override Parameters for EEC Option 1

SSM Override Parameter	Description
ql-dnu	Do Not Use for Synchronization (0xF)
ql-eec1	Synchronous Digital Hierarchy (SDH) Equipment Clock (0xB)
ql-prc	Primary Reference Clock (0x2)
ql-ssu-a	Primary Level Synchronization Supply Unit (0x4)
ql-ssu-b	Second Level Synchronization Supply Unit (0x8)
<input>	Enter SSM as a decimal or hexadecimal value

Table 4. SSM Override Parameters for EEC Option 2

SSM Override Parameter	Description
ql-dus	Do Not Use for Synchronization (0xF)
ql-eec2	Stratum 3 Traceable (0xA)
ql-prov	Provisioned by Network Operator (0xE)
ql-prs	Stratum 1 Traceable (0x1)

Table 4. SSM Override Parameters for EEC Option 2 (Continued)

SSM Override Parameter	Description
ql-smc	SONET Minimum Clock Traceable (0xC)
ql-st2	Stratum 2 Traceable (0x7)
ql-st3e	Stratum 3E Traceable (0xD)
ql-stu	Synchronized Traceability Unknown (0x0)
ql-tnc	Transit Node Clock Traceable (0x4)
<input>	Enter SSM as a decimal or hexadecimal value

SSM override is only configured on those interfaces with SSM enabled. Refer to the command *connect on page 4435*.

Usage Examples

The following example creates an SSM override for EEC option 2, specifically that SSM is provisioned by a network operator:

(config)**#network-sync**
(config-ntwk-sync)**#ssm-override ql-prov**

transmit-ql-threshold <*input*>

Use the **transmit-ql-threshold** command to configure the an upper limit on the value of quality level (QL) transmitted to the user-to-network interfaces (UNIs). Use the **no** form of this command to remove the threshold.

Syntax Description

<*input*>	Specifies the quality level threshold. Refer to the Functional Notes of this command for specifics.

Default Values

By default, this feature is disabled.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The various <*input*> parameters available for QL threshold vary according to the Ethernet equipment clock (EEC) option selected in the Network Sync configuration (refer to the command *eec-option on page 4437*). If you have not specified an EEC option, option 2 is used by default. The following tables outline the <*input*> parameters for the **transmit-ql-threshold** command.

Table 5. Transmit QL Parameters for EEC Option 1

SSM Override Parameter (highest to lowest)	Description
ql-ssu-a	Primary Level Synchronization Supply Unit (0x4)
ql-ssu-b	Secondary Level Synchronization Supply Unit (0x8)
ql-eec1	Synchronous Digital Hierarchy (SDH) Equipment Clock (0xB)
ql-dnu	Do Not Use for Synchronization (0xF)

Table 6. Transmit QL Parameters for EEC Option 2

SSM Override Parameter (highest to lowest)	Description
ql-stu	Synchronized Traceability Unknown (0x0)
ql-st2	Stratum 2 Traceable (0x7)
ql-tnc	Transit Node Clock Traceable (0x4)
ql-st3e	Stratum 3E Traceable (0xD)

Table 6. Transmit QL Parameters for EEC Option 2 (Continued)

SSM Override Parameter (highest to lowest)	Description
ql-eec2	Stratum 3 Traceable (0xA)
ql-dus	Do Not Use for Synchronization (0xF)

Usage Examples

The following example creates a QL threshold for EEC option 2:

(config)**#network-sync**
(config-ntwk-sync)**#transmit-ql-threshold ql-st2**

wait-to-restore *<value>*

Use the **wait-to-restore** command to specify the interval that network synchronization (Network Sync) waits to restore a down clock interface. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the time, in minutes, that Network Sync waits to restore the interface. Valid range is **0** to **31** minutes.

Default Values

By default, the wait-to-restore timer is set to **3** minutes.

Command History

Release R10.11.0	Command was introduced.

Usage Examples

The following example changes the wait-to-restore interval to **10** minutes:

(config)**#network-sync**
(config-ntwk-sync)**#wait-to-restore 10**

OVER-TEMPERATURE PROTECTION COMMAND SET

The AOS over-temperature protection feature provides threshold settings that when reached, allow an AOS unit (that supports the feature) through several precautions to avoid damage due to over heating. When a unit reaches the warning threshold, a Simple Network Management Protocol (SNMP) trap notification is sent to the SNMP host. Once the unit reaches the shutdown threshold, an additional SNMP trap notification is sent, and the unit reboots to a low-power mode. While in low-power mode, only console connections to the unit are allowed. If automatic recovery is disabled, manual intervention is required to recover from the event. The over-temperature protection feature is available on AOS products as outlined in the *AOS Feature Matrix*, available online at https://supportcommunity.adtran.com.

When configuring a recovery threshold or period, be sure to save the configuration changes. If the changes are not saved and the unit reboots due to an over-temperature event, the unit will not automatically recover from low-power mode. Manual intervention will be necessary.

*The recovery and warning thresholds values are stored as Celsius values in AOS. Setting your threshold(s) in Fahrenheit could cause the output of the **show over-temperature protection** command to display a value slightly different from what you entered. This is due to the conversion to Celsius and back to Fahrenheit.*

The recovery and warning thresholds values are stored as Celsius values in AOS. Setting your threshold(s) in Fahrenheit could cause the output of the **show over-temperature protection** command to display a value slightly different from what you entered. This is due to the conversion to Celsius and back to Fahrenheit.

To enter the Over-Temperature Protection Configuration mode, enter the **over-temperature protection** command at the Global Configuration mode prompt, for example:

```
>enable
#configure terminal
(config)#over-temperature protection
(config-over-temp-protection)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

recovery period on page 4447
recovery threshold on page 4448
warning threshold on page 4449

recovery period

Use the **recovery period** command to set a time period for recovery evaluation after an over-temperature event occurs. Use the **no** form of this command to return to the default setting.

Syntax Description

<0-60>	Specifies the amount of time to wait before the unit attempts recovery after an over-temperature event. Valid range is **0** to **60** minutes. A value of **0** will disable the automatic recovery of the unit from low power mode.

Default Values

By default, the recovery threshold period is 15 minutes.

Command History

Release R11.6.0	Command was introduced.

Functional Notes

When a unit exceeds the shutdown temperature threshold, an SNMP trap is sent and the unit is rebooted into a low-power mode. At that point, the recovery period timer begins. Upon completion of the recovery period, the temperature is reevaluated. If the temperature is below the user-defined recovery threshold, the unit will reboot resuming normal operation.

Usage Examples

The following example sets the recovery period for **20** minutes:

(config)**#over-temperature protection**
(config-over-temp-protection)**#recovery period 20**

recovery threshold

Use the **recovery threshold** command to set a recovery threshold temperature for the over-temperature protection feature. Use the **no** form of this command to return to the default setting. Variations of this command include:

recovery threshold <*temp*> **C**
recovery threshold <*temp*> **F**

Syntax Description

<*temp*> **C**	Specifies the recovery temperature threshold. Valid range is **0** to **75** degrees Celsius (C).
<*temp*> **F**	Specifies the recovery temperature threshold. Valid range is **32** to **167** degrees Fahrenheit (F).

Default Values

By default, the recovery threshold temperature is **70 C** (**158 F**).

Command History

Release R11.6.0	Command was introduced.

Functional Notes

When a unit exceeds the shutdown temperature threshold, an SNMP trap is sent and the unit is rebooted into a low-power mode. At that point, the recovery period timer begins. Upon completion of the recovery period, the temperature is reevaluated. If the temperature is below the user-defined recovery threshold, the unit will reboot resuming normal operation.

Usage Examples

The following example sets the recovery threshold to **65** degrees C:

(config)**#over-temperature protection**
(config-over-temp-protection)**#recovery threshold 65 C**

warning threshold

Use the **warning threshold** command to set the temperature threshold to send an SNMP trap during an over-temperature event. Use the **no** form of this command to return to the default setting. Variations of this command include:

warning threshold <*temp*> **C**
warning threshold <*temp*> **F**

Syntax Description

<*temp*> **C**	Specifies the warning temperature threshold. Valid range is **0** to **75** degrees Celsius (C).
<*temp*> **F**	Specifies the warning temperature threshold. Valid range is **32** to **167** degrees Fahrenheit (F).

Default Values

By default, the warning threshold is set to a value of **70 C** (**158 F**).

Command History

Release R11.6.0	Command was introduced.

Functional Notes

Once a unit exceeds the warning temperature threshold, an SNMP trap is sent.

Usage Examples

The following example sets the warning threshold to **70** degrees C:

(config)**#over-temperature protection**
(config-over-temp-protection)**#warning threshold 70 C**

PACKET CAPTURE COMMAND SET

The AOS packet capture feature is used with network monitoring to effectively capture data packets as they traverse the network. As data packets pass through an interface on which the packet capture feature is enabled, a packet-capture monitors the traffic and captures the header and payload of specified packets as they pass through. The captured packets are then exported and stored in either flash memory or CompactFlash storage, and can then be reviewed to determine the cause of network problems, identify security threats, and to maintain efficient data transmission over the network.

In AOS, packet capturing can be attached to one or more interfaces on the device, and can capture Internet Protocol version 4 (IPv4) packets on Layer 3 of the network open systems interconnection (OSI) model. Packet-captures capture both ingress and egress packets on the interface, and can export the captured packets to a Trivial File Transfer Protocol (TFTP) server, flash memory, or CompactFlash memory in libpcap format with a .pcap file extension. Each packet-capture can be limited to only capturing a specified type of traffic by using an access control list (ACL) to specify what type of traffic the packet-capture should capture. The packet-capture works on user-configured size and time limits, which determine when the Pcap file is exported and another capture is initiated. When the size or time limit for a packet-capture expires, the Pcap file is exported. At this point, the limits reset and a new Pcap file is created for subsequently captured packets.

There are two types of packet-captures available in AOS products: a standard packet-capture, and a Session Initiation Protocol (SIP) packet-capture. Standard packet-captures capture packets from all interfaces on which a packet-capture is attached, and archive these captures into a single Pcap file that is exported at regular intervals (based on the packet-capture's size and time limit configuration). The packets captured by standard packet-captures include all ingress and egress IPv4 packets allowed by the ACL associated with the packet-capture, for every interface on which the packet-capture is attached. SIP packet-captures differ from standard packet-captures in that they focus on capturing SIP packets, rather than all allowed IPv4 packets. These packet-captures capture all ingress or egress User Datagram Protocol (UDP) packets that are related to SIP messages, including those related to back-to-back user agent (B2BUA) calls, proxy calls, and messages not related to any call.

For more information about packet capturing, and its implementation and configuration in AOS, refer to the configuration guide *Configuring Packet Capture in AOS*, available online at http://supportforums.adtran.com.

To create a standard packet-capture, and enter the Packet Capture Configuration mode, enter the following command from the Global Configuration mode:

```
(config)#packet-capture 1CAPTURE standard
(config-packet-capture-1CAPTURE)#
```

To create a SIP packet-capture, and enter the Packet Capture Configuration mode, enter the following command from the Global Configuration mode:

```
(config)#packet-capture 1CAPTURE sip
(config-packet-capture-1CAPTURE)#
```


Once you have entered the Packet Capture Configuration mode, you can configure the specific aspects of the packet-capture.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

export on page 4452
limit size <value> on page 4459
limit time <value> on page 4460
match list <ipv4 acl name> on page 4461
max-memory-usage <value> on page 4462
truncate-packet <value> on page 4463

export

Use the **export** command to specify the export mode used to export packet capture (Pcap) files. You can specify the location and type of export used for exporting the Pcap files. Use the **no** form of this command to remove an export entry in the packet-capture configuration. Variations of this command include:

export cflash
export cflash *<path>*

export flash
export flash *<path>*

export usbdrive0
export usbdrive0 *<path>*

export http auto-link
export http auto-link path *<path>*
export http auto-link username *<username>* **password** *<password>*
export http auto-link username *<username>* **password encrypted** *<password>*
export http auto-link port *<port>*
export http auto-link port *<port>* **path** *<path>*
export http auto-link port *<port>* **path** *<path>* **username** *<username>* **password** *<password>*
export http auto-link port *<port>* **path** *<path>* **username** *<username>* **password encrypted** *<password>*
export http auto-link port *<port>* **username** *<username>* **password** *<password>*
export http auto-link port *<port>* **username** *<username>* **password encrypted** *<password>*

export https auto-link
export https auto-link path *<path>*
export https auto-link username *<username>* **password** *<password>*
export https auto-link username *<username>* **password encrypted** *<password>*
export https auto-link port *<port>*
export https auto-link port *<port>* **path** *<path>*
export https auto-link port *<port>* **path** *<path>* **username** *<username>* **password** *<password>*
export https auto-link port *<port>* **path** *<path>* **username** *<username>* **password encrypted** *<password>*
export https auto-link port *<port>* **username** *<username>* **password** *<password>*
export https auto-link port *<port>* **username** *<username>* **password encrypted** *<password>*

export http *<ipv4 address | hostname>*
export http *<ipv4 address | hostname>* **path** *<path>*
export http *<ipv4 address | hostname>* **username** *<username>* **password** *<password>*
export http *<ipv4 address | hostname>* **username** *<username>* **password encrypted** *<password>*
export http *<ipv4 address | hostname>* **port** *<port>*
export http *<ipv4 address | hostname>* **port** *<port>* **path** *<path>*
export http *<ipv4 address | hostname>* **port** *<port>* **path** *<path>* **username** *<username>* **password** *<password>*

export http <*ipv4 address* | *hostname*> **port** <*port*> **path** <*path*> **username** <*username*> **password encrypted** <*password*>
export http <*ipv4 address* | *hostname*> **port** <*port*> **username** <*username*> **password** <*password*>
export http <*ipv4 address* | *hostname*> **port** <*port*> **username** <*username*> **password encrypted** <*password*>

export https <*ipv4 address* | *hostname*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0**
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1**
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-sslv3**
export https <*ipv4 address* | *hostname*> **allow-tls1.1**
export https <*ipv4 address* | *hostname*> **allow-tls1.1 allow-sslv3**
export https <*ipv4 address* | *hostname*> **allow-sslv3**
export https <*ipv4 address* | *hostname*> **path** <*path*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 path** <*path*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 path** <*path*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **allow-tls1.1 path** <*path*>
export https <*ipv4 address* | *hostname*> **allow-tls1.1 allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.1 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.1 allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-sslv3 username** <*username*> **password**

<password>
export https <*ipv4 address* | *hostname*> **allow-tls1.1 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** *<password>*
export https <*ipv4 address* | *hostname*> **allow-sslv3 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 username** <*username*> **password encrypted** *<password>*
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.0 allow-sslv3 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **allow-tls1.1 username** <*username*> **password encrypted** *<password>*
export https <*ipv4 address* | *hostname*> **allow-tls1.1 allow-sslv3 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **allow-sslv3 username** <*username*> **password encrypted** *<password>*
export https <*ipv4 address* | *hostname*> **port** <*port*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0**
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1**
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3**
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-sslv3**
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1**
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 allow-sslv3**
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-sslv3**
export https <*ipv4 address* | *hostname*> **port** <*port*> **path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-sslv3 path** <*path*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **path** <*path*> **username** <*username*> **password** *<password>*
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>

export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-sslv3 path** <*path*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-sslv3 path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 allow-sslv3 path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-sslv3 path** <*path*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-sslv3 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-tls1.1 allow-sslv3 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.0 allow-sslv3 username** <*username*> **password encrypted** <*password*>

export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-tls1.1 allow-sslv3 username** <*username*> **password encrypted** <*password*>
export https <*ipv4 address* | *hostname*> **port** <*port*> **allow-sslv3 username** <*username*> **password encrypted** <*password*>

export tftp <*ipv4 address*>
export tftp <*ipv4 address*> **port** <*port*>

Syntax Description

cflash	Specifies the Pcap files are exported to CompactFlash. If the optional <*path*> parameter is not specified, files are exported to the **/PacketCapture** directory by default.
flash	Specifies the Pcap files are exported to flash memory. If the optional <*path*> parameter is not specified, files are exported to the **/PacketCapture** directory by default.
usbdrive0	Specifies the Pcap files are exported to the USB file system. If the optional <*path*> parameter is not specified, files are exported to the **/PacketCapture** directory by default.
<*path*>	Optional. Specifies a nondefault directory to store the Pcap files when they are exported using CompactFlash, flash, or USB memory. If the optional <*path*> parameter is not specified, files are exported to the **/PacketCapture** directory by default. A specified path can be between **1** and **255** characters in length. Remember that paths must be specified using **/** as the separating character, they must be unescaped, and if they contain spaces, they must be enclosed in quotation marks.
http	Specifies that the Pcap files are exported to a Hypertext Transfer Protocol (HTTP) server.
https	Specifies that the Pcap files are exported to a secure HTTP (HTTPS) server.
allow-tls1.0	Optional. Allows the use of Transport Layer Security protocol version 1.0 when exporting Pcap files. If **allow-tls1.0** is enabled, Secure Socket Layer version 3 (SSLv3) can also optionally be enabled.
allow-tls1.1	Optional. Allows the use of TLS protocol version 1.1 when exporting Pcap files. If **allow-tls1.1** is enabled, SSLv3 can also optionally be enabled.
allow-sslv3	Optional. Allows the use of SSLv3 when exporting Pcap files. If SSLv3 is enabled, TLS version 1.0 is automatically enabled.
auto-link	Specifies that the Pcap files are exported to an auto-link server.
<*ipv4 address* | *hostname*>	Specifies the IPv4 address or host name of the HTTP or HTTPs server to which you are exporting the Pcap files. IPv4 addresses should be expressed in dotted decimal notation, for example, **X.X.X.X**. Host names can be between **4** and **255** characters in length, for example, **hostname.com**.

port <*port*>	Optional. Specifies the port on the HTTP, HTTPS, or Trivial File Transfer Protocol (TFTP) server to which the Pcap files are sent. Valid port range is **1** to **65535**. If no port is specified, the files are sent to the default port of **80** (HTTP), **443** (HTTPS), or UDP port **69** (TFTP). Multiple HTTP(S) exports in the same packet-capture can have the same IPv4 address or host name as long as a different port is specified.
path <*path*>	Optional. Specifies the directory to which the Pcap files are exported. If a path is not specified, the default request path of **/adtran/pcash/aos/receiveCapture/** is used.
username <*username*>	
password <*password*>	Optional. Specifies that basic authentication credentials are sent with every HTTP(S) POST request. User names and passwords can be between **6** and **32** characters in length. User names cannot contain spaces, and if passwords contain spaces, they must be enclosed in quotation marks (for example, **"open sesame"**).
encrypted	Optional. Specifies that the password used in basic authentication for HTTP(S) Pcap file export is encrypted.
tftp <*ipv4 address*>	Specifies that the Pcap files are exported to a TFTP server, and also specifies the IPv4 address of that server. IPv4 addresses should be expressed in dotted decimal notation, for example, **X.X.X.X**.

Default Values

By default, no export location for the Pcap files is configured. When enabled, CompactFlash, flash, and USB exports use the directory **/PacketCapture** by default. When enabled, HTTP, HTTPS, and TFTP exports use the directory **/adtran/pcash/aos/receiveCapture/** by default. When enabled, Pcap files are sent to the default ports of **80** (HTTP), **443** (HTTPS), and UDP port **69** (TFTP).

Command History

Release R10.1.0	Command was introduced.
Release R10.7.0	Command was expanded to include the **auto-link** parameter.
Release R12.3.0	Command was expanded to include the **allow-tls1.0** and **allow-sslv3** parameters.
Release R13.9.0	Command was expanded to include the **allow-tls1.1** parameter.

Usage Examples

The following example specifies that Pcap files are exported to the default directory on the CompactFlash:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#export cflash**

The following example specifies that Pcap files are exported to the packet capture archival server HTTP(S) (PCASH) server at **10.10.2.5** using HTTP with the default directory and port, and without any authentication:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#export http 10.10.2.5**

The following example specifies that the Pcap files are exported to a TFTP server with an IPv4 address of **10.10.5.3**, using the default port:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#export tftp 10.10.5.3**

The following example specifies that the Pcap files are exported to an auto-link server. If a server failover occurs, packet captures exported to an auto-link server can automatically roll over to the new server for export.

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#export http auto-link**

limit size *<value>*

Use the **limit size** command to trigger a packet capture (Pcap) file export after the combined size of all the packet-capture's open captures exceeds the specified size. Use the **no** form of this command to return the maximum open capture size limit to the default value.

Syntax Description

<value>	Specifies the maximum combined size of the packet-capture's open captures. This value can be expressed in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**). Valid range is **0** to **4095M**. If the value is set to **0**, the size limit feature is disabled.

Default Values

By default, the maximum open capture size is set to **1M**.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

At least one capture limit, whether size or time, must be configured with a non-zero value before the packet-capture can be enabled. Configure a size limit using this command, or a time limit using the command *limit time <value> on page 4460*. Adtran recommends that you do not disable packet capture size or time limits.

Usage Examples

The following example changes the maximum combined open capture size limit to **3M**:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#limit size 3M**

limit time *<value>*

Use the **limit time** command to specify the time limit, in seconds, for the packet capture. This command triggers a packet capture (Pcap) file export after the given time value is exceeded. Use the **no** form of this command to return the time limit to the default value.

Syntax Description

<value>	Specifies the capture time limit in seconds. Valid range is **0** to **604800** seconds. Using a value of 0 disables the capture's time limit.

Default Values

By default, Pcap files are set to export after **900** seconds (15 minutes).

Command History

Release R10.1.0	Command was introduced.

Functional Notes

At least one capture limit, whether size or time, must be configured with a non-zero value before the packet-capture can be enabled. Configure a time limit using this command, or a size limit using the command *limit size <value> on page 4459*. Adtran recommends that you do not disable packet capture size or time limits.

Usage Examples

The following example specifies that Pcap files are exported after **2000** seconds:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#time limit 2000**

match list *<ipv4 acl name>*

Use the **match list** command to specify that the packet-capture uses an Internet Protocol version 4 (IPv4) access control list (ACL) to limit the type of traffic that is captured. This command can also be used to prevent feedback, if necessary, or to filter the type of traffic captured for other network management reasons. Use the **no** form of this command to remove the ACL from the packet-capture configuration.

Syntax Description

<ipv4 acl name>	Specifies the name of a previously created IPv4 ACL to use to limit the traffic captured. ACLs are created using the commands *ip access-list extended <ipv4 acl name> on page 1344* or *ip access-list standard <ipv4 acl name> on page 1346*.

Default Values

By default, no ACL is configured or applied to packet-captures.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example applies the previously created IPv4 ACL **PREVENTFEEDBACK** to the packet-capture:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#match list PREVENTFEEDBACK**

max-memory-usage *<value>*

Use the **max-memory-usage** command to specify the maximum memory the packet-capture is allowed to use. This command specifies a memory usage threshold for the capture. Use the **no** form of this command to return the threshold to the default value.

Syntax Description

<value>	Specifies the memory usage threshold in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**). Valid range is **0** to **4294967295** bytes, **0** to **4194303** kilobytes, or **0** to **4095** megabytes.

Default Values

By default, the maximum memory usage threshold is set to **5M**.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

When this threshold is reached, the packet-capture enters memory usage critical (MUC) mode. When in MUC mode, the capture stops capturing packets, continues any ongoing exports, and closes any open captures to begin exporting them. The packet-capture remains in MUC mode until memory usage decreases to 75 percent of the maximum memory usage.

Usage Examples

The following example specifies the maximum memory usage threshold for the packet-capture is **10M**:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#max-memory usage 10M**

truncate-packet <*value*>

Use the **truncate-packet** command to specify the maximum number of bytes to be captured from each packet when using packet capture. This command is primarily used for performance reasons. This command allows you to specify that packets larger than the defined value are truncated. Use the **no** form of this command to return to the truncated packet size default value.

Syntax Description

<*value*>	Specifies the maximum number of captured bytes in a packet before the packet is truncated. This value can be expressed in bytes, kilobytes (**k** or **K**), or megabytes (**m** or **M**).

Default Values

By default, the truncated packet size is set to **0**, which indicates that packets should not be truncated.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example enables packet truncating, and specifies that after **28** bytes the packet is truncated:

(config)**#packet-capture 1CAPTURE standard**
(config-packet-capture-1CAPTURE)**#truncate-packet 28**

QUALITY OF SERVICE MAP COMMAND SET

A quality of service (QoS) policy is defined using a QoS map in the Adtran Operating System (AOS) command line interface (CLI). The QoS map is a named list with sequenced entries. An entry contains a single match reference and one or more actions. To activate the QoS map command set (which allows you to create and/or edit a map), enter a valid version of the **qos map** command at the Global Configuration mode prompt. Multiple map entries for the same QoS map are differentiated by a sequence number. The sequence number is used to assign match order.

Once created, a QoS map must be applied to an interface (using the **qos-policy** command from the desired interface command set) in order to actively process traffic. Any traffic for the interface that does not explicitly match a map entry is sent using the default queuing method for the interface, such as weighted fair queuing (WFQ).

Applying a QoS Map to a PPP or demand interface will cause the interface to drop briefly. This causes a temporary service interruption and the interface should come back up momentarily.

The following example creates and configures a QoS map:

```
>enable
#config terminal
(config)#qos map VOICEMAP 10
(config-qos-map)#match precedence 5
(config-qos-map)#priority 512
(config-qos-map)#exit
(config)#interface fr 1
(config-fr 1)#qos-policy out VOICEMAP
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

bandwidth on page 4466
match on page 4469
match dscp on page 4473
match precedence <value> on page 4477
police cir <rate> on page 4479

bandwidth

Use the **bandwidth** command to specify bandwidth allocation for individual traffic classes for class-based weighted fair queuing (CBWFQ) configurations. Use the **no** form of this command to remove a configured bandwidth allocation. Variations of this command include:

bandwidth <*rate*>
bandwidth <*rate*> **Kbps**
bandwidth <*rate*> **Mbps**
bandwidth percent <*value*>
bandwidth remaining percent <*value*>

Syntax Description

<*rate*>	Allocates the minimum bandwidth for a traffic class, specifying the minimum as an absolute bandwidth in kilobits per second (kbps). Range is **8** to **2000000** kbps.
Kbps	Optional. Indicates the rate specified is in kbps.
Mbps	Optional. Indicates the rate specified is in megabits per second (Mbps).
percent <*value*>	Allocates a minimum bandwidth for a traffic class, specifying the minimum as a percentage of the total interface bandwidth. Refer to *Functional Notes* below for more details.
remaining percent <*value*>	Allocates a minimum bandwidth for a traffic class, specifying the minimum as a percentage of the total interface bandwidth not allocated to priority classes in the quality of service (QoS) map. Refer to *Functional Notes* below for more details.

Default Values

By default, there is no bandwidth allocation configured for a QoS map entry. The bandwidth rate is assumed to be provided in **Kbps** unless **Mbps** is specified.

Command History

Release 10.1	Command was introduced.
Release 17.5	Command was expanded to allow specifying the rate in kbps and Mbps.

Functional Notes

When configuring **bandwidth** allocations for CBWFQ, there are a few rules that must be obeyed.

1. The units of the bandwidth (kbps, Mbps, percent, or remaining percent) must be consistent for all class-based entries (using the **bandwidth** command) in a QoS map set.

2. The total bandwidth between all priority entries (**priority** command) and class-based entries (**bandwidth** command) in a QoS map set should not be configured beyond the specified max-reserved-bandwidth (default 75 percent) on the interface to which the QoS policy is applied (using the **qos-policy** command), or the map will be disabled. In a QoS map, even though limits are defined

regarding consumption of bandwidth by traffic, traffic can burst up to the maximum interface rate when the output queue is not in a congested state. Qos maps are constantly classifying traffic when they are active on an interface, but some of their actions depend on the state of the output queue. When congestion is present, policies defined with the bandwidth command will be limited to the minimum value specified, with excess traffic being queued. During a congested state, policies defined with the priority command will be limited to the maximum value specified, with excess traffic being dropped. Policies defined with the shape or set commands are always enforced regardless of congestion.

When the configured QoS map is applied to a physical interface, AOS displays bandwidth information for the map and the physical interface. For example, if the Frame Relay interface (fr 1) has been connected to the E1 interface (e1 1/1) using the **cross-connect** command, applying the QoS map (MyMapA) to the Frame Relay interface (fr 1) produces the following status message:

2005.08.09 07:28:22 QOS.INTERFACE QOS policy "MyMapA" requires 1288 kbps of bandwidth and 1488 kbps is now available for interface fr 1 -> the QOS policy for this port has been forced ACTIVE.

This status message displays the total of the bandwidths specified in the QoS map (1288 kbps) and the available interface bandwidth using the total line rate configured on the interface (1488 kbps).

3. Up to eight class-based entries (**bandwidth** commands) can be configured in a particular QoS map set.

4. Within a QoS map entry, CBWFQ bandwidth and low latency priority actions are mutually exclusive. However, bandwidth and priority actions may be applied to different entries in the same QoS map.

Determining Bandwidth Entries

*When possible, use the **bandwidth** <value> command to specify an absolute amount of bandwidth (in kbps) for the traffic class.*

When determining the **percent** <*value*> entry, use the following formula:

$$\frac{\text{Bandwidth}}{\text{Line Rate}} \times 100$$

where

Bandwidth	Specifies the minimum amount of bandwidth needed for the traffic (in kbps).
Line Rate	Specifies the total data rate configured on the interface (for example, 8 DS0s (64 kbps per DS0) on a T1 equals a line rate of 512 kbps).

For example, to specify 76.8 kbps of data on an interface with a total of 512 kbps of available bandwidth, and reserving 5 percent of the bandwidth for best effort, routing, and L2 protocol traffic (**max-reserved-bandwidth** = 95) enter the following commands:

(config-qos-map)**#bandwidth percent 15**
(config)**#interface ethernet 0/1**
(config-eth 0/1)**#max-reserved-bandwidth 95**

When determining the **remaining percent** <*value*> entry, use the following formula:

$$\frac{\text{Bandwidth}}{\text{Line Rate}} \times 100$$

where

Bandwidth	Specifies the minimum amount of bandwidth needed for the traffic (in kbps).
Line Rate	Specifies the total data rate configured on the interface (for example, 8 DS0s (64 kbps per DS0) on a T1 equals a line rate of 512 kbps).

For example, to specify 76.8 kbps of data on an interface with a total of 512 kbps of available bandwidth, 256 kbps reserved (using the **priority** command), and reserving 15 percent of the bandwidth for best effort, routing, and L2 protocol traffic (**max-reserved-bandwidth** = 85) enter the following command:

(config-qos-map 1)**#bandwidth remaining percent 45**
(config)**#interface ethernet 0/1**
(config-eth 0/1)**#max-reserved-bandwidth 85**

Usage Examples

The following example creates a QoS map with four traffic classes (based on IP packet precedence values) and allocates bandwidth to each class:

(config)**#qos map MYMAP 1**
(config-qos-map)**#match precedence 5**
(config-qos-map)**#bandwidth percent 25**

(config)**#qos map MYMAP 2**
(config-qos-map)**#match precedence 3**
(config-qos-map)**#bandwidth percent 10**

(config)**#qos map MYMAP 3**
(config-qos-map)**#match precedence 2**
(config-qos-map)**#bandwidth percent 10**

(config)**#qos map MYMAP 4**
(config-qos-map)**#match precedence 1**
(config-qos-map)**#bandwidth percent 15**

match

Use the **match** command to specify which traffic should be processed by this quality of service (QoS) map entry. Use the **no** form of this command to discontinue matching. Variations of this command include:

match any
match fr-dlci *<number>*
match ip list *<ipv4 acl name>*
match ipv6 list *<ipv6 acl name>*
match ip rtp *<port>*
match ip rtp *<begin port> <end port range>*
match ip rtp *<begin port> <end port range>* **all**
match ipv6 rtp *<port>*
match ipv6 rtp *<begin port> <end port range>*
match protocol bridge
match protocol bridge netbeui
match protocol ip
match protocol ipv6
match vlan *<id>*

Syntax Description

any	Match all packets within a QoS map entry that were not matched in previous map entries. Since map entries are processed in the order of their sequence numbers, the **match any** command can be used to process all packets (both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) traffic) not previously matched by a map entry if it is specified as the last QoS map entry.
fr-dlci *<number>*	Match all packets by the specified Frame Relay data link connection identifier (DLCI). Indicate the valid DLCI number from **16** to **1007**.
ip list *<ipv4 acl name>*	Specifies the name of the IPv4 access control list (ACL) you want to use to match packets for this QoS map. Refer to *ip access-list extended <ipv4 acl name> on page 1344* for more information on creating IPv4 ACLs.
ipv6 list *<ipv6 acl name>*	Specifies the name of the IPv6 ACL you want to use to match packets for this QoS map. Refer to *ipv6 access-list extended <ipv6 acl name> on page 1500* for more information on creating IPv6 ACLs.
ip rtp *<port>*	Matches IPv4 Realtime Transport Protocol (RTP) packets with the specified User Datagram Protocol (UDP) destination port.
ip rtp *<begin port> <end port range>*	Matches IPv4 RTP packets with even UDP destination port numbers in the specified range.

all	Optional. Specifies matching all UDP port numbers in the specified range (even and odd). Valid only for **ip rtp** matches.
ipv6 rtp <*port*>	Matches IPv6 RTP packets with the specified UDP destination port.
ipv6 rtp <*begin port*> <*end port range*>	Matches IPv6 RTP packets with even UDP destination port numbers in the specified range.
protocol bridge	Matches frames being bridged by the router.
protocol bridge netbeui	Matches only network basic input/output system (NetBIOS) extended user interface (NetBEUI) frames being bridged by the router.
protocol ip	Matches only IPv4 packets.
protocol ipv6	Matches only IPv6 packets.
vlan <*id*>	Match packets associated with a particular virtual local area network (VLAN). Indicate the VLAN ID number from **1** to **4095**.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.
Release 17.2	Command was expanded to include the **any** and **vlan** <*id*> options.
Release 17.5	Command was expanded to include the **fr-dlci** <*number*> parameter.
Release R10.1.0	Command was expanded to include the **ip list**, **ipv6 list**, **ip rtp**, **ipv6 rtp**, **protocol ip**, and **protocol ipv6** parameters.

Functional Notes

QoS policies are configured in the Adtran Operating System (AOS) command line interface (CLI) to dictate the priority for servicing specified traffic types on a particular interface. QoS policies contain at least one match reference (using the **match** command) and one or more action items (using the **priority**, **bandwidth**, **shape average**, or **set** commands).

The **match** command specifies the criteria used when determining whether incoming traffic is a candidate for the QoS policy action. Multiple **match** statements can exist within the same QoS policy, allowing a single QoS policy to service various types of traffic. You can require *all* of the multiple conditions be met (AND logic) by including the **match-all** parameter when creating the QoS policy. Alternatively, you can choose to include traffic meeting *any* of the conditions (OR logic) by using the **match-any** parameter when creating the QoS policy. Both of these conditions are explained in *qos map <name> <number> on page 1673*.

*Each listed **match** statement is handled independently by the processor. Entering too many **match** statements in a QoS policy can burden the processor.*

For example, consider a network that contains CLASS A and CLASS B traffic (both IPv4 traffic) that each require 25 percent of the total allocated interface bandwidth, the following configuration would be appropriate:

(config)**#qos map MYMAP 10**
(config-qos-map)**#match ip list CLASS_A**
(config-qos-map)**#bandwidth percent 25**

(config)**#qos map MYMAP 20**
(config-qos-map)**#match ip list CLASS_B**
(config-qos-map)**#bandwidth percent 25**

In this example, the combination of both classes will not exceed 25 percent of the total allocated interface bandwidth. CLASS A and CLASS B will share the 25 percent allocation between them. Since there are two match statements in this QoS map entry, traffic can match either IPv4 ACL **CLASS_A** or **CLASS_B** to be processed. By default, this example assumes the **match-any** logic is being applied since it is not specifically configured:

(config)**#qos map MYMAP 10**
(config-qos-map)**#match ip list CLASS_A**
(config-qos-map)**#match ip list CLASS_B**
(config-qos-map)**#bandwidth percent 25**

To remove a configured **match** statement, enter the entire **match** statement with a preceding **no**. For example, to remove the **match** statements from the above configured QoS map:

(config)**#qos map MYMAP 10**
(config-qos-map)**#no match ip list CLASS_A**

and

(config)**#qos map MYMAP 20**
(config-qos-map)**#no match ip list CLASS_B**

Usage Examples

The following example configures QoS for a network with the following needs:

Reserve 15 percent of the line rate for routing IPv4 traffic and L2 protocol traffic (**max-reserved-bandwidth** = 85)

Line Rate = 512 kbps
Guaranteed 256 kbps for Voice
Guaranteed 96 kbps for Class 1
Guaranteed 52 kbps for Class 2

To configure this QoS policy, enter the following QoS map and interface commands:

1. Allocate low latency queuing (LLQ) priority voice traffic.

(config)**#qos map MYMAP 10**
(config-qos-map)**#match ip list VOICE**
(config-qos-map)**#priority 256**

2. Allocate the class-based weighted fair queuing (CBWFQ) data traffic bandwidth for Classes 1 and 2.

(config)**#qos map MYMAP 20**
(config-qos-map)**#match ip list CLASS_1**
(config-qos-map)**#bandwidth 96**

(config)**#qos map MYMAP 30**
(config-qos-map)**#match ip list CLASS_2**
(config-qos-map)**#bandwidth 52**

3. Specify the reserved bandwidth on the appropriate interface and apply the map.

(config-fr 1)**#max-reserved-bandwidth 85**
(config-fr 1)**#qos-policy out MYMAP**

match dscp

Use the **match dscp** command to specify which traffic should be processed by this quality of service (QoS) map based on the differentiated services code point (DSCP) value in the IP header of an Internet Protocol version 4 (IPv4) and/or Internet Protocol version 6 (IPv6) packet. Up to eight DSCP values or identifiers, separated by a space, may be specified in a **match dscp** command. Traffic matching any one of the DSCP values qualifies as a match for the given map entry. Use the **no** form of this command to discontinue matching. Variations of this command include:

match dscp <*value*>
match dscp <*value*> **af***xx*
match dscp <*value*> **cs***x*
match dscp af*xx*
match dscp cs*x*
match dscp default
match dscp ef
match ip dscp <*value*>
match ip dscp <*value*> **af***xx*
match ip dscp <*value*> **cs***x*
match ip dscp af*xx*
match ip dscp cs*x*
match ip dscp default
match ip dscp ef
match ipv6 dscp <*value*>
match ipv6 dscp <*value*> **af***xx*
match ipv6 dscp <*value*> **cs***x*
match ipv6 dscp af*xx*
match ipv6 dscp cs*x*
match ipv6 dscp default
match ipv6 dscp ef

Syntax Description

<*value*>	Specifies the DSCP numeric value. Valid range is **0** to **63**.
af*xx*	Specifies the assured forwarding (AF) class and subclass. Select from: **11** (001010), **12** (001100), **13** (001110), **21** (010010), **22** (010100), **23** (010110), **31** (011010), **32** (011100), **33** (011110), **41** (100010), **42** (100100), or **43** (100110). Up to 8 DSCP values or identifiers may be specified.
cs*x*	Specifies the class selector (CS) value. Valid range is **1** to **7**. Up to 8 DSCP values or identifiers may be specified.
default	Specifies the default DSCP value (000000).
ef	Specifies marking for expedited forwarding (EF).
ip	Specifies the match criteria only apply to IPv4 headers.
ipv6	Specifies the match criteria only apply to IPv6 headers.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release R10.1.0	Command was expanded to include **ip** and **ipv6** parameters to accommodate IPv4 and IPv6 traffic.

Usage Examples

The following example instructs the QoS map named **MYMAP** to match the IPv4 header with a DSCP AF Class 1, Subclass 2 (**af12**):

(config)**#qos map MYMAP 20**
(config-qos-map)**#match ip dscp af12**

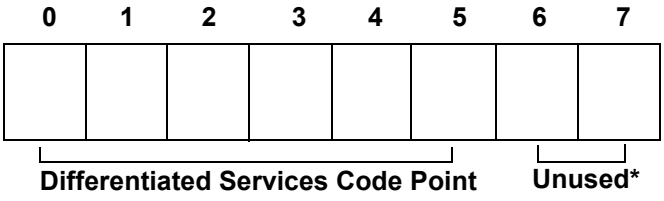
The following example instructs the QoS map named **MYMAP** to match either an IPv4 header or IPv6 header with a DSCP AF Class 1, Subclass 2 (**af12**):

(config)**#qos map MYMAP 20**
(config-qos-map)**#match dscp af12**

Technology Review

The DSCP model was created in RFC 2474 and 2475 to build on the original IPv4 header type of service (ToS) field by creating a 6-bit sequence (combining the precedence value with the delay, throughput, and reliability bits). (IPv6 headers have an 8-bit traffic class field serving the same purpose.) This 6-bit sequence increased the number of available values from 8 to 64. The DiffServ model introduced a new concept to QoS in the IP network environment: per-hop behaviors (PHBs). The PHB premise is that equipment using the DiffServ model have an agreed upon set of rules (PHB types) for handling certain network traffic. Though the RFC explicitly defines what each PHB should be capable of, it does not restrict vendor-specific implementation of the PHBs. Each vendor is free to decide how their network product implements the various defined PHBs.

According to RFC 2474, the differentiated services (DS) field contains the following bits:



*The previously unused bits in the DS field are now used for congestion control and are not discussed in this document.

Equipment following the DiffServ model (DSCP-compliant nodes) must use the entire 6-bit DSCP value to determine the appropriate PHB. The PHBs are defined as the following:

- Default PHB
- Class selector PHB
- Assured forwarding PHB (RFC 2597)
- Expedited forwarding PHB (RFC 2598)

Default PHB

All DSCP-compliant nodes must provide a default PHB to offer best-effort forwarding service. For default PHBs, the DSCP value is 0. Any packet that does not contain a standardized DSCP should be mapped to the default PHB and handled accordingly.

Class Selector PHB

In the class selector PHB, the first three bits in the DSCP value are used for backwards compatibility to systems implementing IP precedence. In this scenario, all but the first three bits of the DS field are set to 0. This compatibility requires DSCP-compliant nodes to provide the same data services as are provided by nodes implementing IP precedence. The following table is a comparison of IP precedence values to their corresponding DSCP values.

IP Precedence Value (bits)	DSCP Value (bits)
0 (000)	0 (000000)
1 (001)	8 (001000)
2 (010)	16 (010000)
3 (011)	24 (011000)
4 (100)	32 (100000)
5 (101)	40 (101000)
6 (110)	48 (110000)
7 (111)	56 (111000)

Assured Forwarding PHB

The flexibility of DiffServ allows for more developed subclasses of service within each main class using the last three bits of the DSCP. As defined in RFC 2597, the assured forwarding PHB creates four main classes of service:

Class	DSCP Bits
AF1	001XX0
AF2	010XX0
AF3	011XX0
AF4	100XX0
X indicates a do not care value.	

The first three bits of the DSCP specify the class and the last bit is always 0. Each class is separated into subclasses using the two remaining bits in the DSCP (bits 3 and 4). The subclasses are divided based on the likelihood that packets in the class are dropped in the event of network congestion. The higher the value for bits 3 and 4, the greater the likelihood that the packets will be dropped.

Bit 3	Bit 4	Drop Precedence
0	1	Low
1	0	Medium
1	1	High

The following table lists the assured forwarding PHB subclasses and their corresponding DSCP bits and values.

Class	Subclass	DSCP Bits	DSCP Value
AF1	1	001010	10
	2	001100	12
	3	001110	14
AF2	1	010010	18
	2	010100	20
	3	010110	22
AF3	1	011010	26
	2	011100	28
	3	011110	30
AF4	1	100010	34
	2	100100	36
	3	100110	38

Expedited Forwarding PHB

RFC 2598 created a new DiffServ PHB intended to provide the best service possible on an IP network. Packets using the expedited forwarding PHB markings should provide service to reduce latency, jitter, and dropped packets, and be guaranteed bandwidth during the entire end-to-end transmission journey through the network. The DSCP value for the expedited forwarding PHB is 46 (DSCP bits are 101110).

match precedence <*value*>

Use the **match precedence** command to specify which traffic should be processed by this quality of service (QoS) map based on the precedence value in the Internet Protocol version 4 (IPv4) and/or Internet Protocol version 6 (IPv6) header of a packet. Use the **no** form of this command to discontinue matching. Variations of this command include:

match precedence <*value*>
match ip precedence <*value*>
match ipv6 precedence <*value*>

Syntax Description

<*value*>	Specifies matching the IP precedence (in numeric value). Valid range is **0** to **7** in ascending order of importance.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release R10.1.0	Command was expanded to include **ip** and **ipv6** parameters to accommodate IPv4 and IPv6 traffic.

Usage Examples

The following example instructs the QoS map named **MYMAP** to match the precedence value of **5** in either IPv4 or IPv6 traffic:

(config)**#qos map MYMAP 20**
(config-qos-map)**#match precedence 5**

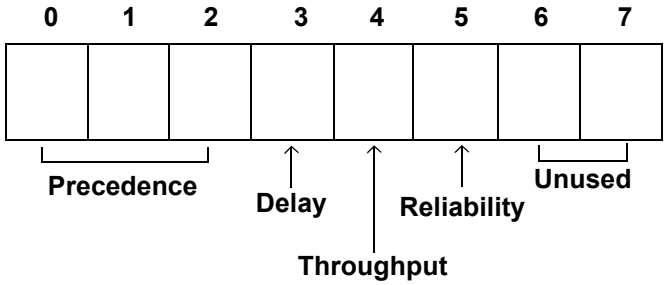
The following example instructs the QoS map named **MYMAP** to match the precedence value of **5** in IPv4 traffic only:

(config)**#qos map MYMAP 20**
(config-qos-map)**#match ip precedence 5**

Technology Review

RFC 791 created a single octet (labeled type of service (ToS) in IPv4 traffic) to help with the difficulty of trying to provide QoS handling in IP networks. IPv6 headers have an 8-bit traffic class field serving the same purpose.

According to RFC 791, the ToS field contains the following bits:



The 3-bit IP precedence values (0 through 7) are specified as:

111	Network Control Packets
110	Internetwork Control Packets
101	Critical Traffic
100	Flash Override
011	Flash
010	Immediate Servicing
001	Priority Traffic
000	Routine Data

The IP precedence values provide network routers with information about what kind of traffic is contained in the IP packet. Based on the IP precedence values, some networks (when supported) can offer special handling to certain packets. In addition, providing IP precedence values to critical traffic (such as route information) ensures that critical packets will always be delivered regardless of network congestion. This traffic is often critical to network and internetwork operation. In general, the higher the IP precedence value, the more important the traffic and the better handling it should receive in the network. It is important to remember that not all equipment in the public IP network will be configured to recognize and handle IP precedence values. While it is a good idea to set the values for important traffic, it does not guarantee special handling.

In addition to the precedence values, RFC 791 specifies bits for delay, throughput, and reliability to help balance the needs of particular traffic types when traveling on the IP network infrastructure. When these bits are set to 0, they are handled with normal operation. When set to 1, each bit specifies premium handling for that parameter. For example, a 1 in the delay position indicates that the traffic is delay sensitive and care should be taken to minimize delay. A 1 in the throughput position indicates that the traffic has higher bandwidth requirements that should be met. A 1 in the reliability position indicates that the traffic is sensitive to delivery issues and care should be taken to ensure proper delivery with all packets of this type. These extra bits are rarely used because they are quite difficult to balance the cost and benefits of each parameter (especially when more than one bit is set to 1).

police cir *<rate>*

Use the **police cir** command to limit the traffic in this quality of service (QoS) map to a specified committed information rate (CIR) threshold and committed burst size (CBS) threshold. If these thresholds are exceeded, the QoS map can drop the traffic. Use the **no** form of this command to disable this feature. Variations of this command include:

police cir *<rate>*
police cir *<rate>* **[count-eth-overhead]**
police cir *<rate>* **cbs** *<size>*
police cir *<rate>* **cbs** *<size>* **[count-eth-overhead]**
police cir *<rate>* **cbs** *<size>* **Bytes [count-eth-overhead]**
police cir *<rate>* **cbs** *<size>* **KB [count-eth-overhead]**
police cir *<rate>* **cbs** *<size>* **MB [count-eth-overhead]**

police cir *<rate>* **bps**
police cir *<rate>* **bps cbs** *<size>*
police cir *<rate>* **bps cbs** *<size>* **Bytes [count-eth-overhead]**
police cir *<rate>* **bps cbs** *<size>* **KB [count-eth-overhead]**
police cir *<rate>* **bps cbs** *<size>* **MB [count-eth-overhead]**
police cir *<rate>* **bps cbs** *<size>* **[count-eth-overhead]**
police cir *<rate>* **bps [count-eth-overhead]**

police cir *<rate>* **Kbps**
police cir *<rate>* **Kbps cbs** *<size>*
police cir *<rate>* **Kbps cbs** *<size>* **Bytes [count-eth-overhead]**
police cir *<rate>* **Kbps cbs** *<size>* **KB [count-eth-overhead]**
police cir *<rate>* **Kbps cbs** *<size>* **MB [count-eth-overhead]**
police cir *<rate>* **Kbps cbs** *<size>* **[count-eth-overhead]**
police cir *<rate>* **Kbps [count-eth-overhead]**

police cir *<rate>* **Mbps**
police cir *<rate>* **Mbps cbs** *<size>*
police cir *<rate>* **Mbps cbs** *<size>* **Bytes [count-eth-overhead]**
police cir *<rate>* **Mbps cbs** *<size>* **KB [count-eth-overhead]**
police cir *<rate>* **Mbps cbs** *<size>* **MB [count-eth-overhead]**
police cir *<rate>* **Mbps cbs** *<size>* **[count-eth-overhead]**
police cir *<rate>* **Mbps [count-eth-overhead]**

Syntax Description

cir <*rate*>	Specifies the CIR for traffic in the QoS map policer entry. This value specifies the average maximum data transmission rate of traffic allowed before the traffic can be dropped. Range is **8192** to **1000000000** bits per second (bps).
bps	Optional. Indicates the rate specified is in bits per second (bps).
Kbps	Optional. Indicates the rate specified is in kilobits per second (kbps).
Mbps	Optional. Indicates the rate specified is in megabits per second (Mbps).
cbs <*size*>	Optional. Specifies the CBS (in bytes) for traffic in this QoS map policer entry. This value specifies the maximum allowable number of bytes transmitted as a burst before the policer drops the traffic. Range is **1600** to **6250000** bytes.
Bytes	Optional. Indicates the burst size specified is in bytes.
KB	Optional. Indicates the burst size specified is in kilobytes (kB).
MB	Optional. Indicates the burst size specified is in megabytes (MB).
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.

Default Values

The default policer CBS rate is specified in **bps**. The default CBS size is specified in **bytes**.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

The policing function of the QoS map cannot be configured with other QoS map features. The QoS map used for traffic policing is applied to the tunnel interface using the command *qos-policy on page 3343*. If other configurations are included in the QoS map when it associated with the tunnel interface, the QoS map association is rejected.

Usage Examples

The following example creates a QoS map for policing traffic with a CIR of **2000** kbps:

(config)**#qos map POLICEQOS1**
(config-qos-map)**#police cir 2000 Kbps**

priority

Use the **priority** command to specify a high-priority queue, prioritizing this traffic above all others. If no traffic is present in any other queue, priority traffic is allowed to burst up to the interface rate; otherwise, priority traffic above the specified bandwidth is dropped. Use the **no** form of this command to disable this feature. Variations of this command include:

priority <*rate*>
priority <*rate*> **strict-rate-limiting**

priority <*rate*> <*burst size*>
priority <*rate*> <*burst size*> **strict-rate-limiting**
priority <*rate*> <*burst size*> **Bytes**
priority <*rate*> <*burst size*> **Bytes strict-rate-limiting**
priority <*rate*> <*burst size*> **KB**
priority <*rate*> <*burst size*> **KB strict-rate-limiting**
priority <*rate*> <*burst size*> **MB**
priority <*rate*> <*burst size*> **MB strict-rate-limiting**

priority <*rate*> **Kbps**
priority <*rate*> **Kbps strict-rate-limiting**
priority <*rate*> **Kbps** <*burst size*>
priority <*rate*> **Kbps** <*burst size*> **strict-rate-limiting**
priority <*rate*> **Kbps** <*burst size*> **Bytes**
priority <*rate*> **Kbps** <*burst size*> **Bytes strict-rate-limiting**
priority <*rate*> **Kbps** <*burst size*> **KB**
priority <*rate*> **Kbps** <*burst size*> **KB strict-rate-limiting**
priority <*rate*> **Kbps** <*burst size*> **MB**
priority <*rate*> **Kbps** <*burst size*> **MB strict-rate-limiting**

priority <*rate*> **Mbps**
priority <*rate*> **Mbps strict-rate-limiting**
priority <*rate*> **Mbps** <*burst size*>
priority <*rate*> **Mbps** <*burst size*> **strict-rate-limiting**
priority <*rate*> **Mbps** <*burst size*> **Bytes**
priority <*rate*> **Mbps** <*burst size*> **Bytes strict-rate-limiting**
priority <*rate*> **Mbps** <*burst size*> **KB**
priority <*rate*> **Mbps** <*burst size*> **KB strict-rate-limiting**
priority <*rate*> **Mbps** <*burst size*> **MB**
priority <*rate*> **Mbps** <*burst size*> **MB strict-rate-limiting**

priority unlimited

priority percent <*value*>
priority percent <*value*> **strict-rate-limiting**

priority percent <*value*> <*burst size*>
priority percent <*value*> <*burst size*> **strict-rate-limiting**
priority percent <*value*> <*burst size*> **Bytes**
priority percent <*value*> <*burst size*> **Bytes strict-rate-limiting**
priority percent <*value*> <*burst size*> **KB**
priority percent <*value*> <*burst size*> **KB strict-rate-limiting**
priority percent <*value*> <*burst size*> **MB**
priority percent <*value*> <*burst size*> **MB strict-rate-limiting**

*The **priority** command cannot be specified in conjunction with the **shape average** command in a quality of service (QoS) entry.*

Syntax Description

<*rate*>	Specifies the bandwidth rate, prioritizing this traffic above all other user traffic. Range is **8** to **1000000** kilobits per second (kbps).
<*burst size*>	Optional. Specifies the maximum burst size (MBS) (in bytes) for traffic in this priority queue. This parameter should be left unconfigured for optimal performance. Range for burst size is **32** to **1000000** bytes.
Kbps	Optional. Indicates the rate specified is in kbps.
Mbps	Optional. Indicates the rate specified is in megabits per second (Mbps).
Bytes	Optional. Indicates the burst size specified is in bytes.
KB	Optional. Indicates the burst size specified is in kilobytes (kB).
MB	Optional. Indicates the burst size specified is in megabytes (MB).
percent <*value*>	Allocates a maximum bandwidth for a traffic class, specifying the maximum as a percentage of the total interface bandwidth. This command is especially useful for protecting bandwidth allocation in multilink applications. Refer to *Functional Notes* for more details.
strict-rate-limiting	Optional. When used with the **priority** command, this feature limits priority traffic to a maximum rate as specified by the <*rate*> variable. When used with **priority percent** command, this feature limits priority traffic to a maximum percentage of the interface bandwidth as specified by the <*value*> variable.
unlimited	Optional. Specifies no limits on the priority queue bandwidth. Use of this feature could potentially use all of the available bandwidth on the interface, even when the **max-reserved-bandwidth** command is not set to 100 percent.

*Use the **priority unlimited** command with extreme caution as it could prevent vital Layer 2 traffic from being processed. A network outage could occur when excessive priority traffic is present and consumes all of the available bandwidth on the interface.*

Default Values

No default values are necessary for this command. The priority rate is assumed to be provided in **Kbps** unless **Mbps** is specified. The burst size is assumed to be provided in bytes unless **KB** or **MB** is specified.

Command History

Release 6.1	Command was introduced.
Release 17.5	Command was expanded to allow specifying the rate in kbps and Mbps. Specifying the burst size in bytes, MB, and kB was also added.
Release 18.1	Command was expanded to include the **strict-rate-limiting** parameter.

Functional Notes

Priority queues are intended for constant bit rate (CBR) traffic, such as voice (due to the rate limiting). Non-CBR traffic typically does not respond well to packet dropping when it is rate limited, so the transfer rate can be much less efficient. Important data traffic should typically use the class-based queue **bandwidth** command (refer to *bandwidth on page 4466*) instead.

The sum of the bandwidths reserved by **priority** and **bandwidth** commands for all entries of a QoS map cannot exceed the available bandwidth on the interface (calculated by the total interface bandwidth minus the **max-reserved-bandwidth** rate specified for the interfaces to which the QoS map is applied). Priority bandwidth is guaranteed bandwidth (in kbps).

Weighted fair queuing (WFQ) must be enabled on an interface to use priority queuing. By default, WFQ is enabled for all interfaces with maximum bandwidth speeds equivalent to T1/E1 and below. It is also employed when shaping is enabled.

Determining Bandwidth Entries

*When possible, use the **priority** <rate> command to specify an absolute amount of bandwidth (in kbps) for the priority queue.*

When determining the **priority percent** <*value*> entry, use the following formula:

$$\frac{\text{Bandwidth}}{\text{Line Rate}} \times 100$$

where

Bandwidth	Specifies the minimum amount of bandwidth needed for the traffic (in kbps).
Line Rate	Specifies the total data rate configured on the interface (for example, 8 DS0s (64 kbps per DS0) on a T1 equals a line rate of 512 kbps).

For example, to specify 76.8 kbps of data on an interface with a total of 512 kbps of available bandwidth, enter the following command:

(config-qos-map 1)**#priority percent 15**

Usage Examples

The following example configures QoS for a network with the following needs:

Reserve 15 percent of the line rate for routing traffic and L2 protocol traffic (**max-reserved-bandwidth** = 85).

Line Rate = 512 kbps
Guaranteed 256 kbps for Voice
Guaranteed 96 kbps for Class 1
Guaranteed 52 kbps for Class 2

To configure this QoS policy, enter the following QoS map and interface commands:

1. Allocate low latency queuing (LLQ) priority voice traffic.

(config)**#qos map MYMAP 10**
(config-qos-map)**#match ip list VOICE**
(config-qos-map)**#priority 256**

2. Allocate the class-based weighted fair queuing (CBWFQ) data traffic bandwidth for CLASS 1 and CLASS 2.

(config)**#qos map MYMAP 20**
(config-qos-map)**#match ip list CLASS_1**
(config-qos-map)**#bandwidth 96**

(config)**#qos map MYMAP 30**
(config-qos-map)**#match ip list CLASS_2**
(config-qos-map)**#bandwidth 52**

3. Specify the reserved bandwidth on the appropriate interface and apply the map.

(config-fr 1)**#max-reserved-bandwidth 85**
(config-fr 1)**#qos-policy out MYMAP**

priority queue-limit *<value>*

Use the **priority queue-limit** command to set the maximum number of packets to store in the priority queue. This command allows the the priority queue to be configured to optimize quality of service (QoS) configurations for higher speed Voice over IP (VoIP) applications. To use this command, you must first enable priority queueing in the QoS map using the command *priority on page 4481*. Use the **no** form of this command to return the queue limit to the default value.

Syntax Description

<value>	Specifies the maximum number of packets to store in the priority queue. Valid range is **256** to **1024** packets.

Default Values

By default, the priority queue limit is set to **256** packets.

Command History

Release R10.3.0	Command was introduced.

Functional Notes

When a priority queue limit is configured on a child QoS map, the parent QoS map's priority queue limit can change. The parent's priority queue limit is based on the the configured priority queue limit for the parent queue, the largest nondefault configured priority queue limit of one of the parent's child QoS map entries, and the default queue limit.

In addition, increasing the priority queue limit also increases the possible latency for priority packets.

Usage Examples

The following example specifies that the priority queue limit for the QoS map **VOICEMAP** is set to **500** packets:

(config)**#qos map VOICEMAP 10**
(config-qos-map)**#priority queue-limit 500**

qos-policy *<map name>*

Use the **qos-policy** command within a parent map to divide a quality of service (QoS) policy map into more specific subclasses. Use the **no** form of this command to remove the subclass and policy mapping attributes of the parent map.

Syntax Description

<map name>	Specifies the QoS map name.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Functional Notes

The **qos-policy** command has two functions in the Adtran Operating System (AOS) command line interface (CLI). In the application described here, it is used to further subdivide a class into more specific subclasses. From the interface configuration command set, it is used to apply a QoS map to the interface. Refer to *qos-policy on page 2306* in the *Ethernet Interface Command Set* for more information on using the **qos-policy** command in the interface configuration command set.

When subdividing a QoS policy map, the most specific (or child map) QoS map should be created first and then the map is referenced using the **qos-policy** command within the QoS map entry of the base map that is being subdivided. The base (or parent map) is applied to the interface using the **qos-policy out** command (refer to *qos-policy on page 2306*).

Only two levels of maps are allowed, meaning child maps (or subclasses) cannot have additional child maps beneath them. A child map cannot reference another child map. If the child map referenced by this command is deleted, then the **qos-policy** command is also deleted from the parent map.

Usage Examples

For example, the following configuration uses the **SHAPEEVCS** QoS map to constrain each VLAN's Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) traffic to specific rates. The virtual local area network (VLAN) 2 traffic that is put into the shaping queue is broken up into class-based queuing (CBQ) or low latency queuing (LLQ) subclasses using the **CLASSQUEUES** QoS map. Traffic not matching a QoS map entry is treated as best effort, and is dynamically assigned to a best effort weighted fair queue (WFQ).

```
(config)#qos map CLASSQUEUES 10
(config-qos-map)#match dscp ef
(config-qos-map)#priority 200
(config-qos-map)#qos map CLASSQUEUES 20
(config-qos-map)#match dscp af31 af32 af33
(config-qos-map)#bandwidth 500          ! class based rate in Kbps
```

(config-qos-map)**#qos map SHAPEEVCS 10**
(config-qos-map)**#match vlan 2**
(config-qos-map)**#shape average 1000000** ! *vlan2Rate in bps*
(config-qos-map)**#qos-policy CLASSQUEUES**

(config-qos-map)**#qos map SHAPEEVCS 20**
(config-qos-map)**#match vlan 3**
(config-qos-map)**#shape average 2000000** ! *vlan3Rate*

(config-qos-map)**#interface eth 0/1**
(config-eth 0/1)**#encapsulation 802.1q**
(config-eth 0/1)**#qos-policy out SHAPEEVCS**

(config-eth 0/1)**#interface eth 0/1.2**
(config-eth 0/1.2)**#vlan-id 2**
(config-eth 0/1.2)**#interface eth 0/1.3**
(config-eth 0/1.3)**#vlan-id 3**

set ce-vlan-pri *<value>*

Use the **set ce-vlan-pri** command to override an Ethernet customer equipment (CE) virtual local area network (VLAN) priority field for the quality of service (QoS) policy map. Use the **no** form of this command to return the priority field value to the default setting.

Syntax Description

<value>	Specifies the CE VLAN priority field value. Valid range is **0** to **7**.

Default Values

By default, the packet's priority value field is not set.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies a CE VLAN priority field value of **3** for **MAP1**:

(config)**#qos map MAP1**
(config-qos-map)**#set ce-vlan-pri 3**

set cos *<value>*

Use the **set cos** command to modify the Layer 2 class of service (CoS) value (on matching packets) to the specified value. Use the **no** form of this command to discontinue the action from the quality of service (QoS) policy map.

Syntax Description

<value>	Specifies the CoS numeric value. Valid range is **0** to **7**.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Functional Notes

QoS policies are configured in the Adtran Operating System (AOS) command line interface (CLI) to dictate the priority for servicing specified traffic types on a particular interface. QoS policies contain at least one match reference (using the **match** command) and one or more action items (using the **priority**, **bandwidth**, **shape**, or **set** commands).

The **set cos** command can be used to change the Ethernet 802.1p priority field for traffic serviced by the QoS policy. Every 802.1q tagged Ethernet frame contains a 3-bit CoS field used for marking data types requiring special handling when traveling through the network.

Usage Examples

The following example sets the CoS value, for all matching traffic within the specified QoS map entry, to **1**:

(config)**#qos map VOICEMAP 10**
(config-qos-map)**#set cos 1**

The following example removes all CoS value change requests from the QoS map entry:

(config)**#qos map VOICEMAP 10**
(config-qos-map)**#no set cos**

set dscp

Use the **set dscp** command to modify the differentiated services code point (DSCP) field (on matching Internet Protocol version 4 (IPv4) and/or Internet Protocol version 6 (IPv6) packets) to the specified value. For more details on determining the DSCP field, refer to the *Technology Review* section of the command *match dscp on page 4473*. Use the **no** form of this command to remove a specified DSCP value. Variations of this command include:

set dscp *<value>*
set dscp af*xx*
set dscp cs*x*
set dscp default
set dscp ef

Syntax Description

<value>	Specifies the DSCP numeric value. Valid range is **0** to **63**.
af*xx*	Specifies the assured forwarding (AF) class and subclass. Select from: **11** (001010), **12** (001100), **13** (001110), **21** (010010), **22** (010100), **23** (010110), **31** (011010), **32** (011100), **33** (011110), **41** (100010), **42** (100100), or **43** (100110).
cs*x*	Specifies the class selector (CS) value. Valid range is **1** to **7**.
default	Specifies the default IP DSCP value (000000).
ef	Specifies marking for expedited forwarding (EF).

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Functional Notes

Quality of service (QoS) policies are configured in the Adtran Operating System (AOS) command line interface (CLI) to dictate the priority for servicing specified traffic types on a particular interface. QoS policies contain at least one match reference (using the **match** command) and one or more action items (using the **priority**, **bandwidth**, **shape**, or **set** commands).

The **set dscp** command can be used to change the differentiated services (DS or DiffServ) field for incoming IPv4 and IPv6 traffic serviced by the quality of service (QoS) policy. Every IPv4 header contains an 8-bit type of service (ToS) field used for marking data types requiring special handling when traveling through the network. IPv6 headers have an 8-bit traffic class field serving the same purpose. Originally this ToS field was used for IP precedence markings (using only the first three bits of the 8-bit field), and was later revised in RFC 2474 to create the 6-bit DS field (reserving the last two bits of the field for future use). The DS field can be manipulated to indicate higher or lower traffic priority using decimal values between 0 and 63.

Usage Examples

This command sets the DSCP value, for all matching traffic within the specified QoS map entry, to **46**:

(config)**#qos map VOICEMAP 10**
(config-qos-map)**#set dscp 46**

set egress-queue <*value*>

Use the **set egress-queue** command to specify the Metro Ethernet network (MEN) egress queue used for traffic that matches the QoS map. Use the **no** form of this command to disable this feature.

Syntax Description

<*value*>	Specifies the MEN egress queue to which the matched traffic is mapped. Valid range is **0** to **7**.

Default Values

By default, this command is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies that traffic matching QoS map **Map1** is queued in MEN egress queue **4**:

(config)**#qos map Map1**
(config-qos-map)**#set egress-queue 4**

set men-c-tag-pri *<priority>*

Use the **set men-c-tag-pri** command to specify the C-tag priority value used for C-tagged egress traffic from a network-to-network interface (NNI) port. Use the **no** form of this command to disable this feature.

Syntax Description

<priority>	Configures the priority for C-tagged egress traffic. Valid range is **0** to **7**.

Default Values

By default, this command is disabled.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

Quality of service (QoS) policies are configured in the Adtran Operating System (AOS) command line interface (CLI) to dictate the priority for servicing specified traffic types on a particular interface. QoS policies contain at least one match reference (using the **match** command) and one or more action items (using the **priority**, **bandwidth**, **shape**, or **set** commands).

The **set men-c-tag-pri** command applies to the C-tag priority of egress traffic from an NNI port. This command overrides the sub-interface's **men-c-tag-pri** setting.

Usage Examples

The following example specifies that C-tagged traffic matching QoS map **Map1** is given a priority of **5**:

(config)**#qos map Map1**
(config-qos-map)**#set men-c-tag-pri 5**

set men-pri *<priority>*

Use the **set men-pri** command to specify the S-tag priority value for S-tagged egress traffic from a network-to-network interface (NNI) port. Use the **no** form of this command to disable this feature.

Syntax Description

<priority>	Configures the priority for S-tagged egress traffic. Valid range is **0** to **7**.

Default Values

By default, this command is disabled.

Command History

Release R10.10.0	Command was introduced.

Functional Notes

Quality of service (QoS) policies are configured in the Adtran Operating System (AOS) command line interface (CLI) to dictate the priority for servicing specified traffic types on a particular interface. QoS policies contain at least one match reference (using the **match** command) and one or more action items (using the **priority**, **bandwidth**, **shape**, or **set** commands).

The **set men-pri** command applies to the S-tag priority of egress traffic from an NNI port. This command overrides the sub-interface's **men-pri** setting.

Usage Examples

The following example specifies that S-tagged traffic matching QoS map **Map1** is given a priority of **5**:

(config)**#qos map Map1**
(config-qos-map)**#set men-pri 5**

set precedence <*value*>

Use the **set precedence** command to modify the precedence value (on matching packets) in the Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) header to the specified value. For more details on precedence, refer to the *Technology Review* section of the command *match precedence <value> on page 4477*. Use the **no** form of this command to discontinue the action from the quality of service (QoS) policy map.

Syntax Description

<value>	Specifies the IP precedence numeric value. Valid range is **0** to **7** in ascending order of importance.

Default Values

No default values are necessary for this command.

Command History

Release 17.2	Command was introduced.

Usage Examples

The following example sets the precedence value, for all matching traffic within the specified QoS map entry, to **1**:

(config)**#qos map VOICEMAP 10**
(config-qos-map)**#set precedence 1**

The following example removes all precedence value change requests from the QoS map entry:

(config)**#qos map VOICEMAP 10**
(config-qos-map)**#no set precedence**

shape average

Use the **shape average** command to shape the traffic in this class to an average rate. Use the **no** form of this command to disable this feature. Variations of this command include:

shape average <*rate*> **[count-eth-overhead]**

shape average <*rate*> **bps**
shape average <*rate*> **bps burst** <*size*>
shape average <*rate*> **bps burst** <*size*> **Bytes [count-eth-overhead]**
shape average <*rate*> **bps burst** <*size*> **KB [count-eth-overhead]**
shape average <*rate*> **bps burst** <*size*> **MB [count-eth-overhead]**
shape average <*rate*> **bps burst** <*size*> **[count-eth-overhead]**
shape average <*rate*> **bps [count-eth-overhead]**

shape average <*rate*> **Kbps**
shape average <*rate*> **Kbps burst** <*size*>
shape average <*rate*> **Kbps burst** <*size*> **Bytes [count-eth-overhead]**
shape average <*rate*> **Kbps burst** <*size*> **KB [count-eth-overhead]**
shape average <*rate*> **Kbps burst** <*size*> **MB [count-eth-overhead]**
shape average <*rate*> **Kbps burst** <*size*> **[count-eth-overhead]**
shape average <*rate*> **Kbps [count-eth-overhead]**

shape average <*rate*> **Mbps**
shape average <*rate*> **Mbps burst** <*size*>
shape average <*rate*> **Mbps burst** <*size*> **Bytes [count-eth-overhead]**
shape average <*rate*> **Mbps burst** <*size*> **KB [count-eth-overhead]**
shape average <*rate*> **Mbps burst** <*size*> **MB [count-eth-overhead]**
shape average <*rate*> **Mbps burst** <*size*> **[count-eth-overhead]**
shape average <*rate*> **Mbps [count-eth-overhead]**

shape average <*rate*> **burst** <*size*> **[count-eth-overhead]**
shape average <*rate*> **burst** <*size*> **Bytes [count-eth-overhead]**
shape average <*rate*> **burst** <*size*> **KB [count-eth-overhead]**
shape average <*rate*> **burst** <*size*> **MB [count-eth-overhead]**

*The **shape average** command cannot be specified in conjunction with the **priority** command in a quality of service (QoS) entry.*

Syntax Description

<rate>	Specifies an average bandwidth. Range is **8192** to **1000000000** bits per second (bps).
burst *<size>*	Optional. Specifies the maximum burst size (MBS) (in bytes) for traffic in this QoS map entry. This parameter should be left unconfigured for optimal performance. Range is **1600** to **6250000** bytes.
count-eth-overhead	Optional. Indicates to include the Ethernet header overhead bytes when determining packet size.
bps	Optional. Indicates the rate specified is in bps.
Kbps	Optional. Indicates the rate specified is in kilobits per second (kbps).
Mbps	Optional. Indicates the rate specified is in megabits per second (Mbps).
Bytes	Optional. Indicates the burst size specified is in bytes.
KB	Optional. Indicates the burst size specified is in kilobytes (kB).
MB	Optional. Indicates the burst size specified is in megabytes (MB).

Default Values

The default shape average rate is specified in **bps**. The default burst size is specified in **bytes**.

Command History

Release 17.2	Command was introduced.
Release 17.5	Command was expanded to allow specifying shape average rate in bps, kbps, and Mbps. Specifying the burst size in bytes, MB, and kB was also added.

Functional Notes

Traffic shaping allows the traffic to be smoothed in order to maintain a uniform rate to take full advantage of the provided bandwidth. Short bursts of traffic above the configured rate are allowed when there is sufficient budget. Traffic outside of the current budget is put into a shaping queue and transmitted once the budget is available.

Usage Examples

The following example shapes the traffic in this QoS class to an average rate of **2000000** bps:

(config)**#qos map VOICEMAP 10**
(config-qos-map)**#shape average 2000000**

RADIUS GROUP COMMAND SET

The remote authentication dial-in user service (RADIUS) Group Command Set details how to create a RADIUS server group and how to add servers to this group. Configured groups of RADIUS servers can be created to be used as methods for authentication, authorization, and accounting (AAA) services in AOS. These subsets are used when defining method lists for AAA actions and can keep you from having to specify that all configured RADIUS servers are used for AAA.

To work with RADIUS server groups, AAA must be enabled. Refer to the command *aaa on on page 1187* for more information. Any RADIUS servers you want to add to the RADIUS server group must already be configured before attempting to add them to the server group. For more information about configuring RADIUS servers, refer to the commands *radius-server on page 1680* and *radius-server host on page 1682*.

RADIUS server groups are first defined in the Global Configuration mode using the **aaa group server** command. Entering this command allows you to create a group of RADIUS servers, and then enters the RADIUS Group Configuration mode in order to add servers to the group. For more information about creating a server group, refer to the command *aaa group server on page 1184*.

For more information about configuring RADIUS server groups for use with AAA, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

To activate the RADIUS Group Configuration mode, enter the **aaa group server radius** <*name*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#aaa group server radius RADAuthgroup
(config-sg-radius)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

server <hostname | ip address> on page 4499
vrf <name> server <hostname | ip address> on page 4501

server <*hostname | ip address*>

Use the **server** command to add a predefined remote authentication dial-in user service (RADIUS) server to the RADIUS server group for use with authentication, authorization, and accounting (AAA). This command applies the configuration to the default unnamed VRF. Use the command *vrf <name> server <hostname | ip address> on page 4501* to apply the configuration to a specific VRF instance. Use the **no** form of this command to remove the server from the group. Variations of this command include:

server <*hostname* | *ip address*>
server <*hostname* | *ip address*> **acct-port** <*number*>
server <*hostname* | *ip address*> **auth-port** <*number*>

Syntax Description

<*hostname*	*ip address*>	Specifies the server to add to the group. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the AOS device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the command *name-server on page 1622*.
acct-port <*number*>	Optional. Specifies the User Datagram Protocol (UDP) port for AAA accounting services with the RADIUS server being added to the RADIUS server group. Port range is **0** to **65535**. This command is reserved for future use. Currently, AOS does not allow RADIUS servers for use with accounting.
auth-port <*number*>	Optional. Specifies the UDP port for AAA authentication services with the RADIUS server being added to the RADIUS server group. Port range is **0** to **65535**.

Default Values

By default, the accounting port is set to **1813** and the authentication port is set to **1812**.

Command History

Release 5.1	Command was introduced.

Functional Notes

Empty RADIUS server groups are not saved. When the last server is removed from a group, AOS automatically deletes the group.

If you choose to change the default authentication port for the RADIUS server, you can then create multiple host entries for the same server. Server groups can have multiple host entries for the same server as long as each entry has a unique identifier (an IP address and a UDP port). If you configure two host entries on the same RADIUS server and are using both host entries for the same service (for example, using both entries for authentication), then the second entry functions as a failover. RADIUS host entries are tried in the order they are configured, so the failover entry is the second configured entry.

For more information about server groups, refer to the command *aaa group server on page 1184*.

Usage Examples

The following example specifies that the RADIUS servers at IP address **192.168.1.2** and **192.168.1.3** are added to the server group **RADAuthgroup**:

(config)**#aaa group server radius RADAuthgroup**
(config-sg-radius)**#server 192.168.1.2**
(config-sg-radius)**#server 192.168.1.3**
(config-sg-radius)**#exit**
(config)**#**

vrf <*name*> server <*hostname | ip address*>

Use the **vrf** <*name*> **server** command to add a predefined remote authentication dial-in user service (RADIUS) server to the RADIUS server group for use with authentication, authorization, and accounting (AAA) on the specified virtual routing and forwarding (VRF) instance. Use the command *server <hostname | ip address> on page 4499* to apply the configuration to the default unnamed VRF instance. Use the **no** form of this command to remove the server from the group. Variations of this command include:

vrf <*name*> **server** <*hostname | ip address*>
vrf <*name*> **server** <*hostname | ip address*> **acct-port** <*number*>
vrf <*name*> **server** <*hostname | ip address*> **auth-port** <*number*>

Syntax Description

<*hostname	ip address*>	Specifies the server to add to the group. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the AOS device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the command *name-server on page 1622*.
acct-port <*number*>	Optional. Specifies the User Datagram Protocol (UDP) port for AAA accounting services with the RADIUS server being added to the RADIUS server group. Port range is **0** to **65535**. This command is reserved for future use. Currently, AOS does not allow RADIUS servers for use with accounting.
auth-port <*number*>	Optional. Specifies the UDP port for AAA authentication services with the RADIUS server being added to the RADIUS server group. Port range is **0** to **65535**.
vrf <*name*>	Specifies the name of the VRF to which to assign the RADIUS server. If no VRF is specified, the association is applied to the default unnamed VRF.

Default Values

By default, the accounting port is set to **1813** and the authentication port is set to **1812**.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Empty RADIUS server groups are not saved. When the last server is removed from a group, AOS automatically deletes the group.

If you choose to change the default authentication port for the RADIUS server, you can then create multiple host entries for the same server. Server groups can have multiple host entries for the same server as long as each entry has a unique identifier (an IP address and a UDP port). If you configure two host entries on the same RADIUS server and are using both host entries for the same service (for example, using both entries for authentication), then the second entry functions as a failover. RADIUS host entries are tried in the order they are configured, so the failover entry is the second configured entry.

For more information about server groups, refer to the command *aaa group server on page 1184*.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example specifies that the RADIUS servers at IP address **192.168.1.2** and **192.168.1.3** on the vrf **RED** are added to the server group **RADAuthgroup**:

(config)**#aaa group server radius RADAuthgroup**
(config-sg-radius)**#vrf RED server 192.168.1.2**
(config-sg-radius)**#vrf RED server 192.168.1.3**
(config-sg-radius)**#exit**
(config)#

SECURITY MONITOR COMMAND SET

The AOS security monitor feature simplifies the collection and display of network information that is relevant to the security of the network. It provides a general overview of network security status that allows the user to quickly and easily assess security threats and firewall status. In the AOS GUI, the security monitor feature is called the security dashboard. For more information about configuring the security monitor feature, refer to the *Security Dashboard* configuration guide available online at https://supportcommunity.adtran.com.

To enter the Security Monitor Configuration mode, enter the **ip security monitor** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip security monitor
(config-secmon)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

cross-connect on page 76
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

color on page 4504
stats-filter <name> on page 4505
threat on page 4506

color

Use the **color** command to display threats in the security monitor using a colored background to correspond to their threat level. Use the **no** version of this command to restore the system default.

Syntax Description

No subcommands.

Default Values

By default, no color is displayed.

Command History

Release 17.5	Command was introduced.

Usage Examples

The following example turns on color in the security monitor:

```
(config-)#ip security monitor
(config-secmon)#color
```

stats-filter <*name*>

Use the **stats-filter** command to apply a previously created security monitor statistics filter globally. Use the **no** version of this command to remove the filter.

Syntax Description

<*name*>	Specifies the filter to be applied.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Functional Notes

A security monitor statistic filter is created from the Global Configuration mode using the command *ip security monitor stats-filter <name> on page 1485*.

Usage Examples

The following example applies a filter named **F1**:

(config-)**#ip security monitor**
(config-secmon)**# stats-filter F1**

threat

Use the **threat** command to define a filter. Use the **no** version of this command to remove all threats from the filter.Variations of this command include:

threat all
threat all except <*id(s)*>
threat add <*id(s)*>
threat add <*id(s)*> **except** <*id(s)*>
threat none
threat remove <*id(s)*>
threat remove <*id(s)*> **except** <*id(s)*>

Syntax Description

all	Adds all security threats to the filter.
<*id(s)*>	Specifies the ID of the security threat.
add	Adds the specified security threats to the filter.
except	Optional. Specifies security threats to be exempted from the filter.
none	Removes all security threats from the filter.
remove	Removes the specified security threats from the filter.

Default Values

No default values are necessary for this command.

Command History

Release 17.5	Command was introduced.

Functional Notes

A list of security threat IDs can be displayed using the command *show ip security on page 780*. The security monitor stats filter is created from the global configuration mode using the command *ip security monitor stats-filter <name> on page 1485*.

Usage Examples

The following example adds all security threats to the filter:

(config-)**#ip security monitor stats-filter F1**
Creating new filter “F1”.
(config-secmon-filter)**#threat all**
(config-secmon-filter)#

TACACS+ GROUP COMMAND SET

The terminal access controller access control system plus (TACACS+) Group Command Set details how to create a TACACS+ server group and how to add servers to this group. Configured groups of TACACS+ servers can be created to be used as methods for authentication, authorization, and accounting (AAA) services in AOS. These subsets are used when defining method lists for AAA actions and can keep you from having to specify that all configured TACACS+ servers are used for AAA.

To work with TACACS+ server groups, AAA must be enabled. Refer to the command *aaa on on page 1187* for more information. Any TACACS+ servers you want to add to the TACACS+ server group must already be configured before attempting to add them to the server group. For more information about configuring TACACS+ servers, refer to the commands *tacacs-server on page 1867* and *tacacs-server host on page 1868*.

TACACS+ server groups are first defined in the Global Configuration mode using the **aaa group server** command. Entering this command allows you to create a group of TACACS+ servers, and then enters the TACACS+ Group Configuration mode in order to add servers to the group. For more information about creating a server group, refer to the command *aaa group server on page 1184*.

For more information about configuring TACACS+ server groups for use with AAA, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

To activate the TACACS+ Group Configuration mode, enter the **aaa group server tacacs+** *<name>* command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#aaa group server tacacs+ TACAuthgroup
(config-sg-tacacs+)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

server <hostname | ip address> on page 4508
vrf <name> server <hostname | ip address> on page 4509

server *<hostname | ip address>*

Use the **server** command to add a predefined terminal access controller access control system plus (TACACS+) server to the TACACS+ server group for use with authentication, authorization, and accounting (AAA). This command applies the configuration to the default unnamed VRF. Use the command *vrf <name> server <hostname | ip address> on page 4509* to apply the configuration to a specific VRF instance. Use the **no** form of this command to remove the server from the group.

Syntax Description

<hostname | ip address>	Specifies the server to add to the group. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the AOS device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the command *name-server on page 1622*.

Default Values

By default, no TACACS+ server groups are configured.

Command History

Release 5.1	Command was introduced.

Functional Notes

Empty TACACS+ server groups are saved. When the last server is removed from a group, AOS automatically maintains the group.

For more information about server groups, refer to the command *aaa group server on page 1184*.

Usage Examples

The following example specifies that the TACACS+ servers at IP address **192.168.1.4** and **192.168.1.5** are added to the server group **TACAuthgroup**:

```
(config)#aaa group server tacacs+ TACAuthgroup
(config-sg-tacacs+)#server 192.168.1.4
(config-sg-tacacs+)#server 192.168.1.5
(config-sg-tacacs+)#exit
(config)#
```

vrf <*name*> server <*hostname | ip address*>

Use the **vrf** <*name*> **server** command to add a predefined terminal access controller access control system plus (TACACS+) server to the TACACS+ server group for use with authentication, authorization, and accounting (AAA) on the specified virtual routing and forwarding (VRF) instance. Use the command *server <hostname | ip address> on page 4508* to apply the configuration to the default unnamed VRF instance. Use the **no** form of this command to remove the server from the group.

Syntax Description

<hostname | ip address>	Specifies the server to add to the group. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the AOS device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the command *name-server on page 1622*.
vrf <*name*>	Specifies the name of the VRF to which to assign the TACACS+ server.

Default Values

By default, no TACACS+ server groups are configured.

Command History

Release R10.7.0	Command was introduced.

Functional Notes

Empty TACACS+ server groups are saved. When the last server is removed from a group, AOS automatically maintains the group.

For more information about server groups, refer to the command *aaa group server on page 1184*.

VRF on AOS products allows a single physical router to be partitioned into multiple virtual routers. Each router instance has its own route table and interface assignments. Beginning with Release 16.1, all AOS routers supporting multiple VRF instances (multi-VRF) have an unnamed default unnamed VRF instance regardless of whether multi-VRF is configured.

Usage Examples

The following example specifies that the TACACS+ servers at IP address **192.168.1.4** and **192.168.1.5** are added to the server group **TACAuthgroup**:

```
(config)#aaa group server tacacs+ TACAuthgroup
(config-sg-tacacs+)#vrf RED server 192.168.1.4
(config-sg-tacacs+)#vrf RED server 192.168.1.5
(config-sg-tacacs+)#exit
(config)#
```

TOP TRAFFIC COMMAND SET

To activate the Top Traffic Configuration mode, enter the **ip flow top-talkers** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip flow top-talkers
(config-top-talkers)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

interval

Use the **interval** command to specify the minimum interval for which Top Talkers data is collected. Use the **no** form of this command to reset the interval to the default value. Variations of this command include:

interval 5
interval 10
interval 15

If the interval is changed after Top Talkers has been enabled, all accumulated data will be lost.

Syntax Description

5	Collects Top Talkers data at **5**-minute intervals.
10	Collects Top Talkers data at **10**-minute intervals.
15	Collects Top Talkers data at **15**-minute intervals.

Default Values

By default, the interval for Top Talkers data collection is set to **5**-minute intervals.

Command History

Release 17.1	Command was introduced.

Functional Notes

When viewing Top Talkers data, the current interval displayed is the interval set with this command. As the specified interval for data accumulation ends, the data is compiled into hourly, 24 hourly, and daily readouts.

Usage Examples

The following example sets the interval for Top Talkers data collection to **10-minute** intervals:

(config)**#ip flow top-talkers**
(config-top-talkers)**#interval 10**

match list *<name>*

Use the **match list** command to specify an access control list (ACL) be used to filter the data that can be used in Top Talkers listings. Use the **no** form of this command to specify no ACL is used and all traffic is considered.

Syntax Description

<name>	Specifies the name of the ACL to be used to filter Top Talkers data collection.

Default Values

By default, no ACL is assigned and all traffic is considered.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example applies the ACL named **engineering** to filter Top Talkers data collection:

(config)**#ip flow top-talkers**
(config-top-talkers)**#match list engineering**

monitor port <*number*> <*description*>

Use the **monitor port** command to add a custom port to the port monitoring list in the Top Talkers feature. Use the **no** form of this command to remove the port from the monitoring list.

Syntax Description

<*number*>	Specifies the port number to be monitored.
<*description*>	Optional. Specifies the application name associated with the port.

Default Values

By default, port monitoring is enabled and monitors well-known Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports when Top Talkers is enabled. Up to 32 custom ports can be added to the port monitoring list.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example adds port **3724**, the World of Warcraft gaming port, to Top Talkers' port monitoring list:

(config)**#ip flow top-talkers**
(config-top-talkers)**#monitor port 3724 World of Warcraft Gaming**

sort-by

Use the **sort-by** command to specify the type of data for the Top Talkers collection. Use the **no** form of this command to return the sorting procedure to the default setting. Variations of this command include the following:

sort-by packets
sort-by bytes

If the statistic to be gathered is changed once Top Talkers is configured, all existing data will be lost.

Syntax Description

packets	Specifies packet statistics are monitored for Top Talkers collection.
bytes	Specifies byte statistics are monitored for Top Talkers collection.

Default Values

By default, Top Talkers will collect **byte** statistics.

Command History

Release 17.1	Command was introduced.

Functional Notes

Data used in the Top Talkers collection can be collected by monitoring the number of packets sent or received or the number of bytes sent or received in a specified amount of time. Collection by byte count and packet count are mutually exclusive and must be configured by the user. Yet each can be helpful depending on specific network needs. Using packet counts to monitor hosts can make it easier to identify the source of problems in cases where a host is infected by a virus, or attacking the network with a port scan. Using byte counts can display overall bandwidth consumption on a host-by-host basis.

Usage Examples

The following example specifies **packet** statistics for collection:

(config)**#ip flow top-talkers**
(config-top-talkers)**#sort-by packets**

top *<number>*

Use the **top** command to specify the number of listings included in the Top Talkers report. Use the **no** form of this command to return to the default value.

If the number of listings is changed after Top Talkers has been enabled, all accumulated data will be lost.

Syntax Description

<number>	Specifies the number of listings shown in the Top Talkers report. Range is **1** to **20**.

Default Values

By default, Top Talkers will display **5** listings in a report.

Command History

Release 17.1	Command was introduced.

Usage Examples

The following example specifies that **10** listings will be included in the Top Talkers report:

(config)**#ip flow top-talkers**
(config-top-talkers)**#top 10**

VOICE COMMAND SETS

The voice command sets are divided into the following sections:

VOICE ACCOUNTS COMMAND SETS

This section includes the following command sets:

VOICE LINE ACCOUNT COMMAND SET

The voice line account commands help you to configure the lines used by voice users. These commands allow you to configure call coverages, call permissions, system activities, and to monitor the quality of the voice connections. Voice line account configurations work hand-in-hand with other voice features, such as system modes, shared line accounts (SLAs), and shared call appearances (SCAs). For more information on system modes, refer to the *NetVanta 7000 Series System Modes* quick configuration guide available online at https://supportcommunity.adtran.com. For more information on SLAs, refer to the *Shared Line Accounts over Analog Trunks* configuration guide, and for more information on SCAs, refer to the *NetVanta 7000 Series Shared Call Appearances* quick configuration guide, both available online at https://supportcommunity.adtran.com.

To create a voice line account and enter the Voice Line Account Configuration mode, enter the **voice line** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice line SALES
(config-SALES)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

accept <template> on page 4520
alc on page 4522
anlp on page 4523
codec-group <name> on page 4524
coverage on page 4525
echo-cancellation on page 4527
held-call-pickup-number <number> on page 4528
member <number> on page 4529
member <number> ring-option <name> on page 4530
nls on page 4531
num-rings <value> on page 4532
password <password> on page 4533
plc on page 4534
reject <template> on page 4535

accept *<template>*

Use the **accept** command to specify numbers that users can dial. This command controls the type of outbound calls users can place. Use the **no** form of this command to remove a configured dial pattern and return to the default setting.

Syntax Description

<template>	Specifies the patterns users can dial. You can enter a complete phone number or wildcards can be used to help define accepted numbers. Refer to *Functional Notes* below for more information on using wildcards.

Default Values

By default, the cost value is **zero**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.

2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.

3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].

4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example allows users on the line **SALES** to dial any local number:

(config)**#voice line SALES**
(config-SALES)**#accept Nxxxxxx**

alc

Use the **alc** command to enable auto level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example activates the ALC for line **SALES**:

(config)**#voice line SALES**
(config-SALES)**#alc**

anlp

Use the **anlp** command to enable advanced nonlinear processing which adds attenuation of residual echo level by way of a nonlinear processor (NLP) placed in the send path of an echo canceller. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **anlp** is disabled.

Command History

Release A4.08	Command was introduced.

Usage Examples

The following example enables anlp:

```
(config)#voice line SALES
(config-SALES)#anlp
```

codec-group *<name>*

Use the **codec-group** command to specify the coder-decoder (CODEC) list to be used by this account. Use the **no** form of this command to remove the CODEC list from the account.

Syntax Description

<name>	Specifies the CODEC list to be used for this account.

Default Values

By default, no CODEC lists are assigned.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the integrated services digital network (ISDN) trunk.
Release 15.1	Command was added to the Voice Line Configuration command set.
Release A1	Command was included in the Voice Loopback Account Configuration command set.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) Configuration command set.

Functional Notes

The **codec-group** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation, and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893.*

Usage Examples

The following example applies the CODEC list **List1** to the voice line **sales**:

(config)**#voice line sales**
(config-sales)**#codec-group List1**

coverage

Use the **coverage** command to configure call coverage parameters for the line. The call coverage setting determines how a call is handled if the party dialed does not answer after a specified number of rings. Use the **no** form of this command to remove an individual coverage parameter. Variations of this command include:

coverage aa
coverage aa <*number*>
coverage internal <*number*> **num-rings** <*value*>
coverage operator
coverage operator num-rings <*value*>
coverage override <*value*>
coverage vm
coverage vm <*number*>
coverage <*system mode*> **aa**
coverage <*system mode*> **aa** <*number*>
coverage <*system mode*> **external** <*number*>
coverage <*system mode*> **internal** <*number*>
coverage <*system mode*> **internal** <*number*> **num-rings** <*value*>
coverage <*system mode*> **operator**
coverage <*system mode*> **operator num-rings** <*value*>
coverage <*system mode*> **vm**
coverage <*system mode*> **vm** <*number*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
aa	Forwards the call to the default auto attendant.
aa <*number*>	Forwards the call to a specific extension programmed for the auto attendant. If no extension is specified, the phone is forwarded to the default auto attendant.
external <*number*>	Forwards the call to the specified external number. If no number is entered, the default auto answer is used.
internal <*number*>	Forwards the call to the specified internal number.
num-rings <*value*>	Optional. Specifies the number of rings for the call before performing the next action. Valid range is **1** to **9**.
operator	Forwards the call to the operator.
override <*value*>	Ignores the programmed system mode schedule.
vm	Forwards the call to voicemail.
vm <*number*>	Optional. Forwards the call to the specified mailbox number.

Default Values

By default, no call coverage is specified.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was updated to include the voicemail and number of rings options.
Release 12.1	Command was updated to include the auto attendant, global, and operator options.
Release A1	Command was updated to include the system mode feature options.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

Usage Examples

The following example specifies that the line be forwarded after **3** rings to the internal extension **8500** when in the **night** system mode:

(config)**#voice line sales**
(config-sales)**#coverage night internal 8500 num-rings 3**

echo-cancellation

Use the **echo-cancellation** command to improve voice quality for packetized-based voice calls, such as Voice over Internet Protocol (VoIP) or Media Gateway Control Protocol (MGCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **echo-cancellation** is enabled.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example activates **echo-cancellation** for voice line **sales**:

(config)**#voice line sales**
(config-sales)**#echo-cancellation**

held-call-pickup-number <*number*>

Use the **held-call-pickup-number** <*number*> command to configure an extension to dial to retrieve a call that is put on hold by the shared line appearance (SLA). Use the **no** version of this command to remove the number.

Syntax Description

<*number*>	Specifies the extension to dial to retrieve SLA calls put on hold.

Default Values

No default values are necessary for this command.

Command History

Release R10.6.0	Command was introduced.

Usage Examples

The following example configures **6535** as the held call pickup number for SLA **SALES**:

(config)**#voice line SALES**
(config-SALES)**#held-call-pickup-number 6535**

member <*number*>

Use the **member** command to add members to a voice shared line appearance (SLA). Use the **no** version of this command to remove the member from the SLA.

Syntax Description

<*number*>	Specifies the extension of the member to be added to the SLA.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example adds extension **6535** as a member of the SLA:

(config)**# voice line SALES**
(config-SALES)**#member 6535**

member <*number*> ring-option <*name*>

Use the **member** <*number*> **ring-option** command to assign a ring option to a member of the specified voice shared line appearance (SLA). Use the **no** version of this command to remove the ring option from the member.

Syntax Description

<*number*>	Specifies the extension of the member to be configured.
<*name*>	Specifies the name of the ring option to apply to the SLA member.

Default Values

No default values are necessary for this command.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example assigns ring option **NORM** to the **6535,** which is a member of the SLA **SALES**:

(config)**#voice line SALES**
(config-SALES)**#member 6535 ring-option NORM**

nls

Use the **nls** command to enable the non-linear suppression (NLS) option for the line. This option sets the echo canceller to reduce acoustic echo. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example enables NLS for voice line **SALES**:

```
(config)#voice line SALES
(config-SALES)#nls
```

num-rings <*value*>

Use the **num-rings** command to specify the number of rings for call pickup before the system redirects the call. Each system mode call coverage action can be configured with a different number of rings based on preference. Use the **no** form of this command to return to the default setting. Variations of this command include:

num-rings <*value*>
num-rings <*system mode*> <*value*>
num-rings override <*value*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
override	Ignores the programmed system mode schedule.
<*value*>	Specifies the number of rings before the next action. The valid range is **1** to **9**.

Default Values

By default, **num-rings** is set to **4**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was updated to include the system mode feature options.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

Usage Examples

The following example sets the number of rings for voice line **SALES** to **6**:

(config)**#voice line SALES**
(config-SALES)**#num-rings 6**

password *<password>*

Use the **password** command to create a password or personal identification number (PIN) to protect voice settings and messages. Use the **no** form of this command to remove a password.

*The password configured must be used when configuring the IP phone using the **IP Phone Configs** Web-based graphical user interface (GUI) menu.*

Syntax Description

<password>	Specifies a 4-digit password or PIN.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example sets the password for voice line **SALES** to **4321**:

(config)**#voice line SALES**
(config-SALES)**#password 4321**

plc

Use the **plc** command to enable packet loss concealment (PLC). PLC is used to prevent choppy connections by concealing a packet loss by replacing the lost packet with another voice packet in the data stream. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, PLC is enabled.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example disables PLC for the voice line **SALES**:

(config)**#voice line SALES**
(config-SALES)**#no plc**

reject *<template>*

Use the **reject** command to specify numbers users cannot dial on the line. This feature allows administrators to restrict callers from unwanted outbound calls, such as international calls and 900 numbers. Use the **no** form of this command to disable this feature.

Syntax Description

<template>	Specifies the patterns that users cannot dial on the line. You can enter a complete phone number or wildcards can be used to help define rejected numbers. Refer to *Functional Notes* below for more information on using wildcards. For example, you can enter **900$** to prevent users from dialing all 900 numbers.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example blocks calls to any 900 number on the line **SALES**:

(config)**#voice line SALES**
(config-SALES)**#reject 1900$**

rtp delay-mode

Use the **rtp delay-mode** command to configure the Realtime Transport Protocol (RTP) jitter buffer packet delay mode settings. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Use the **no** form of this command to return to the default setting. Variations of this command include:

rtp delay-mode adaptive
rtp delay-mode fixed

Syntax Description

adaptive	Configures the RTP jitter buffer packet delay to adjust during a call based on network conditions.
fixed	Configures the RTP jitter buffer packet delay to remain constant.

Default Values

By default, the RTP delay mode is set to **adaptive**. This allows for minimal latency by adjusting the average packet delay based on the conditions of the network.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example configures RTP delay mode as fixed:

(config)**#voice line SALES**
(config-SALES)**#rtp delay-mode fixed**

rtp dtmf-relay

Use the **rtp dtmf-relay** command to configure the method by which Realtime Transport Protocol (RTP) dual tone multi-frequency (DTMF) events are relayed. The dial digits can be sent inband or out-of-band (OOB) of the voice stream. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp dtmf-relay inband
rtp dtmf-relay nte <*value*>

Syntax Description

inband	Specifies that RTP DTMF events be relayed inband in the RTP stream.
nte <*value*>	Specifies that RTP DTMF events be relayed OOB using named telephone events (NTEs). Enter an NTE value between **96** and **127**.

Default Values

By default, the **rtp dtmf-relay** is set for **NTE 101**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example configures RTP DTMF relay events for **inband**:

(config)**#voice line SALES**
(config-SALES)**#rtp dtmf-relay inband**

rtp frame-packetization <*value*>

Use the **rtp frame-packetization** command to configure the Realtime Transport Protocol (RTP) frame packetization time in milliseconds for individual trunks and users. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP frame packetization time value in milliseconds. Select from **10**, **20**, **30**, or **40** milliseconds.

Default Values

By default, the **rtp frame-packetization** time is set to **20** milliseconds on all trunks and users.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release R10.8.0	Command was expanded to include **40** milliseconds.

Usage Examples

The following example sets the frame packetization time for voice line **SALES** to **10** milliseconds:

(config)**#voice line SALES**
(config-SALES)**#rtp frame-packetization 10**

rtp packet-delay

Use the **rtp packet-delay** command to configure the maximum Realtime Transport Protocol (RTP) packet delays. This command is used to set the allowable limits of latency on the network. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp packet-delay maximum <*value*>
rtp packet-delay nominal <*value*>

Syntax Description

maximum <*value*>	Sets the maximum delay time value in increments of **10** milliseconds. Range is **40** to **320** milliseconds.
nominal <*value*>	Sets the nominal delay time value in increments of **10** milliseconds. Range is **10** to **240** milliseconds.

Default Values

By default, the RTP packet delay for maximum is **100**, and for nominal is **50**.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example configures the RTP maximum delay time on voice line SALES to **200** milliseconds:

(config)**#voice line SALES**
(config-SALES)**#rtp packet-delay maximum 200**

rtp qos dscp <*value*>

Use the **rtp qos dscp** command to configure the maximum Realtime Transport Protocol (RTP) quality of service (QoS) parameters for differentiated services code point (DSCP). Use the **no** form of this command to return to the default global value.

Syntax Description

<*value*>	Configures the RTP QoS parameter for DSCP. Enter a value between **0** and **63**.

Default Values

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. The default global DSCP value for RTP is **46**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Functional Notes

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. QoS is set using a DSCP value. Valid DSCP values are **0** to **63**, and a higher DSCP value has a higher priority. The default global DSCP value for RTP is **46**. Remember that if you are using a public IP connection, such as the Internet, for Voice over Internet Protocol (VoIP), end-to-end QoS may not be guaranteed. The default DSCP value for Session Initiation Protocol (SIP) is **26**. To configure QoS for the RTP traffic that carries the voice conversation, use the command **ip rtp qos dscp** followed by the desired DSCP value.

Usage Examples

The following example configures the RTP QoS DSCP for voice line SALES to **60**:

(config)**#voice line SALES**
(config-SALES)**#rtp qos dscp 60**

seize-timeout <*seconds*>

Use the **seize-timeout** command to specify the maximum time the trunk will be seized before placing a call. Use the **no** form of this command to return to the default timeout interval.

Syntax Description

<*seconds*>	Specifies maximum number of seconds the trunk will be seized before placing a call. Valid range is **5** to **120** seconds.

Default Values

By default, the **seize-timeout** period is set to **30** seconds.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets the **seize-timeout** period to **20** seconds:

(config)**#voice line SALES**
(config-SALES)**#seize-timeout 20**

sip-keep-alive

Use the **sip-keep-alive** command to configure the type of keep-alive method for this Session Initiation Protocol (SIP) trunk. Keep-alive messages must be sent between SIP device and the registrar to keep the connected channel open for communication. Use the **no** form of this command to return to disable this feature. Variations of this command include the following:

sip-keep-alive info
sip-keep-alive info <*value*>
sip-keep-alive options
sip-keep-alive options <*value*>

Syntax Description

info	Specifies the INFO method to be used for the keep-alives on the trunk.
options	Specifies the OPTIONS method to be used for the keep-alives on the trunk.
<*value*>	Optional. Specifies the amount of time in seconds between the type of SIP keep-alive messages being sent during a call. Range is **30** to **3600** seconds.

Default Values

By default, **sip-keep-alive** is set to **info 60** on NetVanta 7000 Series products. For IP business gateways (Total Access 900(e) Series and NetVanta 6000 Series) **sip-keep-alive** is disabled by default.

Command History

Release 13.1	Command was introduced
Release A2.04	Command was added to the Voice Line and Voice User command sets.

Usage Examples

The following example sets the keep-alive method to **info**:

(config)**#voice line SALES**
(config-SALES)**#sip-keep-alive info**

trunk <*Txx*>

Use the **trunk** command to specify the trunk the voice line will use. Use the **no** form of this command to remove a configured trunk group.

Syntax Description

<*Txx*>	Specifies an ID number for the trunk. The trunk ID is in the format Txx, where xx is the trunk ID number. Enter a trunk ID between **1** and **99**. For example, trunk **T02**.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example adds trunk **T02** to the voice line SALES:

(config)**#voice line SALES**
(config-SALES)**#trunk t02**

vad

Use the **vad** command to enable voice activity detection (VAD). VAD blocks out noise categorized as silence during a voice connection. The silent voice packets are not transmitted, allowing bandwidth usage to be reduced. Although VAD saves bandwidth, the quality of the voice call may be compromised. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, VAD is enabled for all T1 robbed-bit signaling (RBS) trunks and users.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.

Usage Examples

The following example disables VAD on voice line SALES:

(config)**#voice line SALES**
(config-SALES)**#no vad**

VOICE LOOPBACK ACCOUNT COMMAND SET

A loopback account is an internal account that creates a Realtime Transport Protocol (RTP) loopback. Loopback calls allow you to actively troubleshoot voice issues. Loopback calls can be originated from the command line interface (CLI), or the configured loopback extension can automatically answer an incoming call. During the loopback call, you hear a mirror copy of the transmitted audio path. The loopback call gives you the ability to verify two-way audio, test latency, and judge call quality. Unlike normal calls between two endpoints, statistics are not recorded on loopback calls. Since the audio in the call is simply a retransmission of the RTP stream, the call is not handled by digital signal processor (DSP) so information on packet loss, delay, and jitter are not available on loopback calls.

In order to place loopback calls, you will need to configure a loopback extension. This is a special type of user account that the AOS unit will use to place and/or receive the actual loopback call. A loopback extension has the same basic configurable options that affect call quality as a normal user account. Loopback accounts also require the same configuration that any other user account would need in order to properly interact with the Session Initiation Protocol (SIP) server, SIP identity, external caller ID override, etc. A dial plan must also be configured for the loopback account. The dial plan is needed for the unit to accept and route the call. The commands in this section are used for creating and configuring a loopback account. For additional information about configuring loopback accounts, refer to the *Configuring the AOS Voice Loopback Account* configuration guide available online at https://supportcommunity.adtran.com.

To create a loopback account and enter the Voice Loopback Account Configuration mode, enter the **voice loopback** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice loopback 5555
(config-LB-5555)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

alc

Use the **alc** command to enable auto level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example activates ALC for loopback **5555**:

(config)**#voice loopback 5555**
(config-LB-5555)**#alc**

appearances *<value>*

Use the **appearances** command to specify the number of simultaneous loopback calls allowed on the system. The maximum number of calls allowed is five. Use the **no** form of this command to reset the number of call appearances allowed on this account.

Syntax Description

<value>	Configures the number of calls. Range is **1** to **5**.

Default Values

By default, the call appearances is set to **1**.

Command History

Release A1	Command was introduced.

Usage Examples

The following example specifies that **3** simultaneous loopback calls be allowed on the system:

(config)**#voice loopback 5555**
(config-LB-5555)**#appearances 3**

caller-id

Use the **caller-id** command to specify a name or number to display as the caller ID information. Use the **no** form of this command to return to the default value. Variations of this command include:

caller-id name <*name*>
caller-id number <*number*>

Syntax Description

name <*name*>	Specifies the name of the loopback account.
number <*number*>	Specifies the number of the loopback account.

Default Values

By default, the caller ID will display the extension number used when creating the loopback account. If no **name** or alternate **number** is specified, the loopback extension number will be displayed.

Command History

Release A1	Command was introduced.

Usage Examples

The following example sets the caller ID information for the loopback account:

(config)**#voice loopback 5555**
(config-LB-5555)**#caller-id name VQMTesting**
(config-LB-5555)**#caller-id number 372-5555**

codec-list *<name>*

Use the **codec-list** command to specify the coder-decoder (CODEC) list to be used by this account. This CODEC can be used for normal voice traffic or for Session Border Controller (SBC) transcoding. Use the **no** form of this command to remove the CODEC list from the account. Variations of this command include:

codec-list *<name>*
codec-list *<name>* **both**
codec-list *<name>* **in**
codec-list *<name>* **out**
codec-list any
codec-list any both
codec-list any in
codec-list any out

Syntax Description

<name>	Specifies the CODEC list to be used for this account.
any	Specifies that any possible CODEC is allowed on this account.
both	Optional. Specifies that the CODEC list is applied to both transmitted and received Session Description Protocol (SDP) transmissions.
in	Optional. Specifies that the CODEC list is applied to received SDP only.
out	Optional. Specifies that the CODEC list is applied to transmitted SDP only.

Default Values

By default, no CODEC lists are assigned.

Command History

Release R10.4.0	Command was introduced and replaced the **codec-group** command.

Functional Notes

The **codec-list** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893*.

In addition, CODEC lists can be used for the SBC transcoding feature. For more information about this feature, its uses, and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

> NOTE *Because you can choose to specify that any CODEC is used by a Session Initiation Protocol (SIP) endpoint with the **any** keyword, do not create a CODEC list with the name of **any**.*

Usage Examples

The following example applies the CODEC list **LIST1** to incoming SDP traffic on loopback account **5555**:

(config)#**voice loopback 5555**
(config-LB-5555)#codec-list LIST1 in

echo-cancellation

Use the **echo-cancellation** command to improve voice quality for packetized-based voice calls, such as Voice over Internet Protocol (VoIP) or Media Gateway Control Protocol (MGCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **echo-cancellation** is enabled.

Command History

Release 9.3	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example activates **echo-cancellation** for loopback **5555**:

(config)**#voice loopback 5555**
(config-LB-5555)**#echo-cancellation**

media-loopback

Use the **media-loopback** command to designate a voice loopback account to be used for media loopback. Media loopback enables media sessions to be established where the media is looped back to the transmitter. This is typically referred to as active monitoring of services. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **media-loopback** is disabled.

Command History

Release A4.03	Command was introduced.

Usage Examples

The following example configures voice loopback account **5555** to be used for media loopback:

```
(config)#voice loopback 5555
(config-LB-5555)#media-loopback
```

nls

Use the **nls** command to enable the non-linear suppression (NLS) option for the user. This option sets the echo canceller to reduce acoustic echo. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example enables NLS for loopback **5555**:

(config)**#voice loopback 5555**
(config-LB-5555)**#nls**

num-rings <*value*>

Use the **num-rings** command to specify the number of rings before the loopback account answers (when called). Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the number of rings before answering. Specify **0** through **9** rings. Entering **0** specifies answering the call immediately.

Default Values

By default, **num-rings** is set to **0**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example sets the number of rings for loopback **5555** to **3**:

(config)**#voice loopback 5555**
(config-LB-5555)**#num-rings 3**

plc

Use the **plc** command to enable packet loss concealment (PLC). PLC is used to prevent choppy connections by replacing a lost packet with another voice packet in the data stream. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, PLC is enabled.

Command History

Release 11.1	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example disables PLC for loopback **5555**:

(config)**#voice loopback 5555**
(config-LB-5555)**#no plc**

rtp delay-mode

Use the **rtp delay-mode** command to configure the Realtime Transport Protocol (RTP) jitter buffer packet delay mode settings. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Use the **no** form of this command to return to the default setting. Variations of this command include:

rtp delay-mode adaptive
rtp delay-mode fixed

Syntax Description

adaptive	Configures the RTP jitter buffer packet delay to adjust during a call based on network conditions.
fixed	Configures the RTP jitter buffer packet delay to remain constant.

Default Values

By default, the RTP delay mode is set to **adaptive**. This allows for minimal latency by adjusting the average packet delay based on the conditions of the network.

Command History

Release 11.1	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example configures the RTP delay mode as fixed:

(config)**#voice loopback 5555**
(config-LB-5555)**#rtp delay-mode fixed**

rtp dtmf-relay

Use the **rtp dtmf-relay** command to configure the method by which Realtime Transport Protocol (RTP) dual tone multi-frequency (DTMF) events are relayed. The dial digits can be sent inband or out-of-band (OOB) of the voice stream. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp dtmf-relay inband
rtp dtmf-relay nte <*value*>

Syntax Description

inband	Specifies that RTP DTMF events be relayed inband in the RTP stream.
nte <*value*>	Specifies that RTP DTMF event value be relayed OOB using named telephone events (NTEs). Enter a named telephone event (NTE) value between **96** and **127**.

Default Values

By default, the **rtp dtmf-relay** is set for **nte 101**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example configures RTP DTMF relay events for **inband**:

(config)**#voice loopback 5555**
(config-LB-5555)**#rtp dtmf-relay inband**

rtp frame-packetization <*value*>

Use the **rtp frame-packetization** command to configure the Realtime Transport Protocol (RTP) frame packetization time in milliseconds for individual trunks and users. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP frame packetization time value in milliseconds. Select from **10**, **20**, **30**, or **40** milliseconds.

Default Values

By default, the **rtp frame-packetization** time is set to **20** milliseconds on all trunks and users.

Command History

Release 9.3	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.
Release R10.8.0	Command was expanded to include **40** milliseconds.

Usage Examples

The following example sets the frame packetization time for loopback account **5555** to **10** milliseconds:

(config)**#voice loopback 5555**
(config-LB-5555)**#rtp frame-packetization 10**

rtp packet-delay

Use the **rtp packet-delay** command to configure the maximum Realtime Transport Protocol (RTP) packet delays. This command is used to set the allowable limits of latency on the network. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp packet-delay fax <*value*>
rtp packet-delay maximum <*value*>
rtp packet-delay nominal <*value*>

Syntax Description

fax <*value*>	Sets the fax delay time value in milliseconds. Range is **0** to **500** milliseconds.
maximum <*value*>	Sets the maximum delay time value in increments of 10 milliseconds. Range is **40** to **320** milliseconds.
nominal <*value*>	Sets the nominal delay time value in increments of 10 milliseconds. Range is **10** to **240** milliseconds.

Default Values

By default, the RTP packet delays are **fax 300**, **maximum 100**, and **nominal 50**.

Command History

Release 11.1	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example configures the RTP fax delay time for loopback **5555** to **200** milliseconds:

(config)**#voice loopback 5555**
(config-LB-5555)**#rtp packet-delay fax 200**

rtp qos dscp <*value*>

Use the **rtp qos dscp** command to configure the Realtime Transport Protocol (RTP) differentiated services code point (DSCP) value. Use the **no** form of this command to return to the default global value.

Syntax Description

<*value*>	Configures the RTP value for DSCP. The DSCP values are **0** to **63**.

Default Values

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. The default global DSCP value for RTP is **46**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Functional Notes

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. QoS is set using a DSCP value. Valid DSCP values are **0** to **63**, and a higher DSCP value has a higher priority. The default global DSCP value for RTP is **46**. Remember that if you are using a public IP connection, such as the Internet, for Voice over Internet Protocol (VoIP), end-to-end QoS may not be guaranteed. The default DSCP value for Session Initiation Protocol (SIP) is **26**. To configure QoS for the RTP traffic that carries the voice conversation, use the command **ip rtp qos dscp** followed by the desired DSCP value.

Usage Examples

The following example sets the RTP quality of service (QoS) DSCP value to **14**:

(config)**#voice loopback 5555**
(config-LB-5555)**#rtp qos dscp 14**

sip-identity

Use the **sip-identity** command to configure the Session Initiation Protocol (SIP) registration options for the user. Use the **no** form of this command to disable the setting. Variations of this command include the following:

sip-identity <*station*> <*Txx*>
sip-identity <*station*> <*Txx*> **register**
sip-identity <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

<*station*>	Specifies the station to be used for SIP trunk (e.g., **station extension**).
<*Txx*>	Specifies the SIP trunk through which to register the server. The trunk is specified in the format Txx (e.g., **T01**).
register	Registers the user to the server.
auth-name <*username*>	Optional. Sets the user name that will be required as authentication for registration to the SIP server.
password <*password*>	Optional. Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release A1	Command was included in the Voice Loopback Account Configuration command set.

Usage Examples

The following example specifies trunk **T02** and extension **4400** for SIP identity on the loopback account:

(config)**#voice loopback 5555**
(config-LB-5555)**#sip-identity 4400 T02**

VOICE USER ACCOUNT COMMAND SET

Voice user accounts are used to define phone users that are registered to an AOS voice product. There are three different types of user accounts: Session Initiation Protocol (SIP), analog, and virtual. SIP user accounts are associated with a SIP user agent. Analog user accounts are user accounts that are associated with a physical foreign exchange station (FXS) interface. Virtual user accounts are not associated with a physical port. These user types can be used for special applications such as forwarding calls.

The commands in this section describe how to configure voice features for user accounts. For more information about configuring voice users, refer to the configuration guide *Configuring User Accounts on the NetVanta 7000 Series* available online at https://supportcommunity.adtran.com.

To create a user account and enter the Voice User Account Configuration mode, enter the **voice user** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice user 4444
(config-4444)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

All other commands for this command set are described in this section in alphabetical order.

alc

Use the **alc** command to enable automatic level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature. Variations of this command include:

alc
alc level -16
alc level -17
alc level -18
alc level -19
alc level -20
alc level -21
alc level -22

Syntax Description

level -16	Optional. Specifies the ALC attenuation level is -16 dBm0.
level -17	Optional. Specifies the ALC attenuation level is -17 dBm0.
level -18	Optional. Specifies the ALC attenuation level is -18 dBm0.
level -19	Optional. Specifies the ALC attenuation level is -19 dBm0.
level -20	Optional. Specifies the ALC attenuation level is -20 dBm0.
level -21	Optional. Specifies the ALC attenuation level is -21 dBm0.
level -22	Optional. Specifies the ALC attenuation level is -22 dBm0.

Default Values

By default, ALC is disabled.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.
Release A2.04	Command was expanded to include the **level** parameters.

Usage Examples

The following example activates the ALC for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#alc**

billing-codes

Use the **billing-codes** command to specify that billing codes are allowed or required for all external calls on the voice user account. Using the **no** form of this command indicates billing codes are not allowed on the account. Variations of this command include:

billing-codes allowed
billing-codes required

Syntax Description

allowed	Specifies that billing codes are allowed for external calls on the user account.
required	Specifies that billing codes are required for external calls on the user account.

Default Values

By default, billing codes are not used.

Command History

Release R10.3.0	Command was introduced.

Usage Examples

The following example specifies that billing codes are required for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#billing-codes required**

block-caller-id

Use the **block-caller-id** command to block all inbound caller ID delivery to this user. This command prevents the selected user from receiving caller ID information. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example activates the **block-caller-id** command for user **4444**:

(config)**#voice user 4444**
(config-4444)**#block-caller-id**

busy-out alert-mode

Use the **busy-out alert-mode** command to specify the busy-out monitoring alert mode received by the voice user when attempting to make a call when the voice trunk is in busied out mode. Use the **no** form of this command to return to the default busy-out alert mode. Variations of this command include:

busy-out alert-mode fast-busy
busy-out alert-mode no-battery
busy-out alert-mode no-dialtone

Syntax Description

fast-busy	Specifies that a fast busy tone is heard on the port when the voice trunk is in busied out mode.
no-battery	Specifies the battery is removed from the port when the voice trunk is in busied out mode.
no-dialtone	Specifies there is no dialtone on the port when the voice trunk is in busied out mode.

Default Values

By default, the busy-out alert is set to **no-dialtone**.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example specifies the busy-out alert type as **fast-busy** for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#busy-out alert-mode fast-busy**

busy-out monitor track <*name*>

Use the **busy-out monitor track** command to enable busy-out monitoring on the port used by this voice user. Use the **no** version of this command to disable the busy-out monitoring feature.

Syntax Description

<*name*>	Specifies a track to associate with the voice port for busy-out monitoring use.

Default Values

By default, busy-out monitoring is not enabled on the port.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example enables busy-out monitoring and associates the track **TESTTRACK** with the port used by voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#busy-out monitor track TESTTRACK**

caller-id-override

Use the **caller-id-override** command to manipulate caller ID information for the user. This command is used to conceal user's name and number or to display a different name and number for internal or external caller ID. Use the **no** form of this command to disable this feature. Variations of this command include:

caller-id-override emergency-number <*number*>
caller-id-override external-number <*number*>
caller-id-override external-name <*name*>
caller-id-override external-name empty
caller-id-override internal-name empty
caller-id-override internal-name <*name*>
caller-id-override internal-number empty
caller-id-override internal-number <*number*>

Syntax Description

emergency-number <*number*>	Replaces the caller ID number on emergency calls with the specified number.
external-number <*number*>	Replaces the caller ID number on external calls with the specified number.
external-name <*name*>	Replaces the caller ID name on external calls with the specified name.
internal-name <*name*>	Replaces the caller ID name on internal calls with the specified name.
internal-number <*number*>	Replaces caller ID number on internal calls with the specified number.
empty	Makes the caller ID name or number on internal calls and the caller ID name on external calls display as blank.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release A4.01	Command was expanded to include the **emergency-number** and **external-name** parameters.

Usage Examples

The following example activates the **caller-id-override** command for external numbers for user **4444**:

(config)**#voice user 4444**
(config-4444)**#caller-id-override external-number 256-555-8000**

This example activates the **caller-id-override** command for names with internal calls and makes the display appear blank:

(config)**#voice user 4444**
(config-4444)**#caller-id-override internal-number empty**

call-waiting

Use the **call-waiting** command to enable call waiting for a user. The selected user will be allowed to receive caller ID information. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example activates the **call-waiting** command for user **4444**:

```
(config)#voice user 4444
(config-4444)#call-waiting
```

codec-list *<name>*

Use the **codec-list** command to specify the coder-decoder (CODEC) list to be used by this account. This CODEC can be used for normal voice traffic or for Session Border Controller (SBC) transcoding. Use the **no** form of this command to remove the CODEC list from the account. Variations of this command include:

codec-list *<name>*
codec-list *<name>* **both**
codec-list *<name>* **in**
codec-list *<name>* **out**
codec-list any
codec-list any both
codec-list any in
codec-list any out

Syntax Description

<name>	Specifies the CODEC list to be used for this account.
any	Specifies that any possible CODEC is allowed on this account.
both	Optional. Specifies that the CODEC list is applied to both transmitted and received Session Description Protocol (SDP) transmissions.
in	Optional. Specifies that the CODEC list is applied to received SDP only.
out	Optional. Specifies that the CODEC list is applied to transmitted SDP only.

Default Values

By default, no CODEC lists are assigned.

Command History

Release R10.4.0	Command was introduced and replaced the **codec-group** command.

Functional Notes

The **codec-list** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893***.**

In addition, CODEC lists can be used for the SBC transcoding feature. For more information about this feature, its uses, and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

> NOTE *Because you can choose to specify that any CODEC is used by a Session Initiation Protocol (SIP) endpoint with the **any** keyword, do not create a CODEC list with the name of **any**.*

Usage Examples

The following example applies the CODEC list **LIST1** to incoming SDP traffic for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#codec-list LIST1 in**

connect

Use the **connect** command to associate physical ports with the user. This command assigns a specific station or port type to the user. Use the **no** form of this command to remove associations. Variations of this command include:

connect fxs <*slot/port*>
connect sip

Syntax Description

fxs <*slot/port*>	Specifies that a foreign exchange station (FXS) port is associated with the user.
sip	Specifies that this is a Session Initiation Protocol (SIP) user.

Default Values

By default, users are not associated with physical ports.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example associates the physical FXS slot 1/port 1 interface with the user **4444**:

(config)#**voice user 4444**
(config-4444)#**connect fxs 1/1**

The following example associates a SIP port with the user **4444**.

(config)#**voice user 4444**
(config-4444)#**connect sip**

contact-group *<group number>*

Use the **contact-group** command to create a FindMe-FollowMe contact group for the user and enter the group's configuration mode. Using the **no** form of this command removes the contact group from the user's configuration.

Syntax Description

<group number>	Specifies the contact group number. Valid range is **1** to **5**.

Default Values

By default, no contact groups are configured.

Command History

Release A4.01	Command was introduced.

Functional Notes

FindMe-FollowMe must be enabled on the user account to use configured contact groups. FindMe-FollowMe is enabled using the command *findme-followme on page 4593*.

Each contact group is numbered, and group numbers specify which contact group FindMe-FollowMe searches first. For example, the calling party number will be matched to the permitted calling party number list in contact group 1 before contact group 2. If a match is found, the actions for contact group 1 are performed. Otherwise, the next contact group is searched for matches. Each user account can have up to **5** contact groups.

The **contact-group** command creates a FindMe-FollowMe contact group and enters the group's configuration mode. Commands in this configuration mode are detailed in the section *FindMe-FollowMe Contact Group Command Set on page 4752*.

Usage Examples

The following example creates contact group **1** for voice user **4444**, and enters the group's configuration mode:

```
(config)#voice user 4444
(config-4444)#contact-group 1
(config-4444-cg-1)#
```

cos

Use the **cos** command to set class of service (CoS) mode for the user. The CoS can be set to change for the user based on the current system mode by including the system mode parameter. The CoS defines the types of phone service that will be available to the user during the time period. Use the **no** form of this command to disable this feature. Variations of this command include:

cos <*name*>
cos <*system mode*> <*name*>
cos no-access
cos <*system mode*> **no-access**
cos override <*name*>
cos override no-access

Syntax Description

<*name*>	Specifies the predefined CoS.
<*system mode*>	Optional. Specifies the system mode to configure. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
no-access	Blocks users from placing calls when the CoS is applied.
override	Ignores the programmed system mode schedule.

Default Values

By default, the CoS is set to **no-access**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was expanded to include the system mode options.

Functional Notes

Additional functionality for this feature is provided by assigning a CoS to a specific system mode. When the system mode changes at a trigger point, the user's CoS changes.

For example, a CoS applied to the user when the system mode is specified as **night** can be used to prevent outbound calls during evening hours. System modes are defined from the Global Configuration mode using the command *voice system-mode on page 1971*.

Usage Examples

The following example specifies the CoS **Assistant** for the user **4444**.

(config)**#voice user 4444**
(config-4444)**#cos Assistant**

The following example configures the user's CoS to change to **general** when the system mode changes to **night**.

(config)**#voice user 4444**
(config-4444)**#cos night general**

coverage

Use the **coverage** command to configure call coverage parameters for the user. The call coverage setting determines how a call is handled if the dialed party does not answer after a specified number of rings. Use the **no** form of this command to remove an individual coverage parameter. Variations of this command include:

coverage aa
coverage aa <*number*>
coverage findme-followme
coverage global <*name*>
coverage internal <*number*>
coverage internal <*number*> **num-rings** <*value*>
coverage operator
coverage operator num-rings <*value*>
coverage override external <*number*>
coverage override global <*name*>
coverage override internal <*number*>
coverage override internal <*number*> **num-rings** <*value*>
coverage override operator
coverage override operator num-rings <*value*>
coverage override vm
coverage override vm <*number*>
coverage vm
coverage vm <*number*>
coverage <*system mode*> **aa**
coverage <*system mode*> **aa** <*number*>
coverage <*system mode*> **external** <*number*>
coverage <*system mode*> **findme-followme**
coverage <*system mode*> **global** <*name*>
coverage <*system mode*> **internal** <*number*>
coverage <*system mode*> **internal** <*number*> **num-rings** <*value*>
coverage <*system mode*> **operator**
coverage <*system mode*> **operator num-rings** <*value*>
coverage <*system mode*> **vm**
coverage <*system mode*> **vm** <*number*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
aa	Forwards the call to the default auto attendant.
aa <*number*>	Forwards the call to a specific extension programmed for the auto attendant. If no extension is specified, the phone is forwarded to the default auto attendant.

external <*number*>	Forwards the call to the specified external number. If no number is entered, the default auto answer is used.
findme-followme	Specifies that FindMe-FollowMe is the preferred coverage type for this user.
global <*name*>	Uses the specified global call coverage list.
internal <*number*>	Forwards the call to the specified internal number.
num-rings <*value*>	Optional. Specifies the number of rings for the call before performing the next action. Valid range is **1** to **9**.
operator	Forwards the call to the operator.
override	Ignores the programmed system mode schedule.
vm	Forwards the call to voicemail.
vm <*number*>	Optional. Forwards the phone to the specified mailbox number.

Default Values

By default, no system mode call coverage is specified.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was updated to include the **voicemail** and **num-rings** parameters.
Release 12.1	Command was updated to include the **aa**, **global**, and **operator** parameters.
Release A1	Command was updated to include the system mode feature options.
Release A4.01	Command was updated to include the **findme-followme** parameter.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

The FindMe-FollowMe feature can be used instead of other call coverages. When FindMe-FollowMe is enabled as the call coverage mode, incoming callers are directed according to the user's configuration of the FindMe-FollowMe feature. For more information about configuring FindMe-FollowMe, refer to the commands *contact-group <group number> on page 4577* and *findme-followme on page 4593*, as well as to the command sets *FindMe-FollowMe Contact Group Command Set on page 4752* and *FindMe-FollowMe Action Script Command Set on page 4744*. If you would like more information about FindMe-FollowMe, its configuration, and how it relates to call coverage, refer to the *Configuring User Accounts on the NetVanta 7000 Series* quick configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the user's phone be forwarded to the internal extension **8500** when in the **night** system mode after **3** rings.

(config)**#voice user 4444**
(config-4444)**#coverage night internal 8500 num-rings 3**

The following example specifies that incoming calls to the user extension **4444** follow the call coverage outlined in the user's FindMe-FollowMe configuration:

(config)**#voice user 4444**
(config-4444)**#coverage findme-followme**

did <*number*>

Use the **did** command to configure direct inward dialing (DID) parameters for the extension. DID is used if a service provider is providing digits to the unit on inbound calls or if the unit needs to provide DID information to a piece of customer premises equipment (CPE). Use the **no** form of this command to disable this feature.

Syntax Description

<*number*>	Specifies the DID number for the user.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example assigns a **did** number of **555-4560** to user **4444**:

(config)**#voice user 4444**
(config-4444)**#did 5554560**

directory-include

Use the **directory-include** command to add this user in a dial-by-name (DBN) directory. Adding users to the directory allows the users to call parties by the voice user's name stored in the system. Use the **no** form of this command to disable this feature. Variations of this command include:

directory-include
directory-include first-name <*name*>
directory-include first-name <*name*> **last-name** <*name*>
directory-include <*directory name*>
directory-include <*directory name*> **first-name** <*name*>
directory-include <*directory name*> **first-name** <*name*> **last-name** <*name*>

Syntax Description

first-name <*name*>	Optional. Specifies the directory entry of the user's first name to be included in the directory.
last-name <*name*>	Optional. Specifies the directory entry of the user's last name to be included in the directory.
<*directory name*>	Optional. Specifies the name of a directory.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 14.1	Command was expanded.

Functional Notes

Using this command automatically retrieves the values stored in the **first-name** and **last-name** for the DBN directory. If a user also uses an alias, you may add extra entries into the DBN directory by specifying the first and last names within the **directory-include** command.

By default, a system directory is always available. All voice users are automatically added as members of the system directory.

Usage Examples

The following example adds the user **4444** to a DBN directory:

(config)**#voice user 4444**
(config-4444)**#directory-include**

dnd

Use the **dnd** command to enable the do-not-disturb (DND) option for the user. This setting prevents the phone extension assigned to the user from ringing. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example enables DND for user **4444**:

(config)**#voice user 4444**
(config-4444)**#dnd**

dnis-digits <*value*>

Use the **dnis-digits** command to enable the dialed number identification service (DNIS) delay feature and to specify the number of DNIS dual tone multi-frequency (DTMF) digits that are outpulsed to the terminal when a call is routed to an automatic call distributor (ACD), such as a fax server, that is connected to a foreign exchange station (FXS) port. For more information on how this feature works, refer to the *Functional Notes* and *Technology Review* sections below. Use the **no** form of this command to disable the DNIS delay feature. Variations of this command include:

dnis-digits <*value*>
dnis-digits <*value*> **digit-delay** <*value*>
dnis-digits <*value*> **digit-delay** <*value*> **cut-through-delay** <*value*>

Syntax Description

dnis-digits <*value*>	Specifies the number of DNIS digits that are to be outpulsed. Range is **1** to **16** digits.
digit-delay <*value*>	Optional. Specifies the delay (in milliseconds) between the terminal going off-hook and the first DNIS digit outpulse. The delay is specified in **100** ms increments and the range is **100** to **1000** ms.
cut-through-delay <*value*>	Optional. Specifies the delay (in milliseconds) between the outpulsing of the final DNIS digit and the start of two-way voice traffic. The delay is specified in **100** ms increments and the range is **100** to **2000** ms.

Default Values

By default, this feature is disabled and zero DNIS digits are outpulsed. When the shortest version of the command is used (**dnis-digits** <*value*>), the digit delay is set to **200** ms and the cut-through-delay is set to **500** ms by default.

Command History

Release A2.04	Command was introduced.

Functional Notes

The DNIS delay feature is used when an FXS port is connected to an ACD, such as a fax server. When the switchboard routes a call to the port and the terminal answers, the trailing digits of the called number are outpulsed to allow the terminal to finish routing the call. The **dnis-digits** command allows you to configure how many digits are outpulsed. For more information on how the feature operates, refer to the *Technology Review* section of this command.

This feature is available only when the voice user type is specified as FXS.

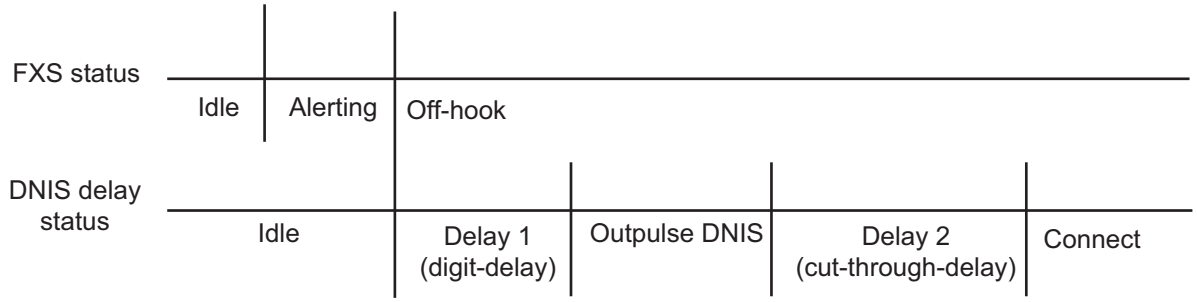
Usage Examples

The following example specifies that the voice user's terminal outpulse **4** DNIS digits and use the delay default values (**200** ms for **digit-delay** and **500** ms for **cut-through-delay**):

(config)**#voice user 4444**
(config-4444)**#dnis-digits 4**

Technology Review

The following diagram demonstrates the actions taken by the FXS port and the DNIS delay feature:



The diagram shows that the DNIS feature is idle while the FXS port is alerting and waiting for the terminal to go off-hook. After the terminal is off-hook, the DNIS feature enters the Delay 1 state, specified by the **digit-delay** parameter of this command. Entering this state allows sufficient time for any transients audible on the two-way wire to die away, and for the terminal to attach a digit register. After Delay 1 times out, DNIS DTMF digits are outpulsed to the terminal. The feature then enters the Delay 2 state, specified by the **cut-through-delay** parameter of this command. Entering this state allows for the connected terminal to finish routing the call. Once the feature enters the Connect state, a two-way voice band connection is established. Using the **dnis-digits** command allows you to specify the number of DNIS digits outpulsed and the duration of both delay periods in this process.

This feature is intended for use with a fax server, where multiple inbound fax numbers are all routed to a single analog port. To use this feature effectively, follow these steps:

1. Create a voice user account using the command *voice user <extension> on page 1983*. The extension number assigned can be arbitrary, or it can be one of the desired inbound fax lines.

2. Connect an analog port using the command *connect on page 4576*.

3. Assign an alias for each inbound fax line to be steered into the fax server using the command *alias "<text>" on page 75*.

4. Set the number of DNIS digits using the dnis-digits command. These digits must be set in conjunction with the fax server configuration.

The configuration of the DNIS digits feature appears as follows:

(config)**#voice user 4444**
(config-4444)**#connect fxs 0/1**
(config-4444)**#description “fax-server”**
(config-4444)**#alias 2565552081**
(config-4444)**#alias 2565552082**
(config-4444)**#alias 2568882093**
(config-4444)**#alias 2568882094**
(config-4444)**#dnis-digits 7**
(config-4444)**#exit**

door-phone

Use the **door-phone** command to enable the door phone mode for this extension. Use the **no** form of this command to disable the door phone mode for this extension.

Syntax Description

No subcommands.

Default Values

By default, the door phone mode is disabled.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example makes extension **4444** the door phone extension.

(config)**#voice user 4444**
(config-4444)**#door-phone**

echo-cancellation

Use the **echo-cancellation** command to improve voice quality for packetized-based voice calls, such as Voice over Internet Protocol (VoIP) or Media Gateway Control Protocol (MGCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **echo-cancellation** is enabled.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example activates **echo-cancellation** for user **4444**:

```
(config)#voice user 4444
(config-4444)#echo-cancellation
```

email <*address*>

Use the **email** command to configure the primary email notification address for this extension. Use the **no** form of this command to remove a configured email address.

Syntax Description

<*address*>	Specifies the primary email notification address for this extension.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the primary email notification address for this extension as **first.last@company.com**.

(config)**#voice user 4444**
(config-4444)**#email first.last@company.com**

email-secondary *<address>*

Use the **email-secondary** command to configure the secondary email notification address for this extension. The secondary email address will be used based on the email notification schedule. Use the **no** form of this command to remove a configured secondary email address.

Syntax Description

<address>	Specifies the secondary email notification address for this extension.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the secondary email notification address for this extension as **first.last@company.com**.

(config)**#voice user 4444**
(config-4444)**#email-secondary first.last@company.com**

findme-followme

Use the **findme-followme** command to enable the FindMe-FollowMe feature for the user. Use the **no** form of this command to disable the feature. Variations of this command include:

findme-followme
findme-followme enhanced

Syntax Description

enhanced	Optional. Specifies that the enhanced version of FindMe-FollowMe is enabled on the user account.

Default Values

By default, FindMe-FollowMe is disabled.

Command History

Release A4.01	Command was introduced.

Functional Notes

The **enhanced** version of FindMe-FollowMe allows the AOS device to remain in the talk path only for external calls with press-to-accept enabled.

FindMe-FollowMe is a complex feature requiring a large amount of system resources. Decreasing the amount of enhanced FindMe-FollowMe can reduce the amount of system resources used by the feature.

This command must be enabled on the user account for additional FindMe-FollowMe configurations. For more information about configuring the FindMe-FollowMe feature, refer to *FindMe-FollowMe Contact Group Command Set on page 4752* and *FindMe-FollowMe Action Script Command Set on page 4744*, or the *Configuring User Accounts for the NetVanta 7000 Series* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables the basic FindMe-FollowMe feature for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#findme-followme**

findme-followme caller-id-override external-number *<name/number>*

Use the **findme-followme caller-id-override external-number** command to specify if caller ID override will be used on the voice user's account for FindMe-FollowMe calls. This command allows the user to specify the inbound caller ID and name when external FindMe-FollowMe calls are received. Use the **no** version of this command to disable the caller ID override on the voice user's FindMe-FollowMe settings.

Syntax Description

<name/number>	Specifies the external number (up to 16 digits) to use in the caller ID.

Default Values

By default, FindMe-FollowMe caller ID override is disabled.

Command History

Release R10.2.0	Command was introduced.

Functional Notes

FindMe-FollowMe must be enabled on the user account using the command *findme-followme on page 4593* before configuring FindMe-FollowMe caller ID override.

For more information about configuring the FindMe-FollowMe feature, refer to *FindMe-FollowMe Contact Group Command Set on page 4752* and *FindMe-FollowMe Action Script Command Set on page 4744*, or the *Configuring User Accounts on the NetVanta 7000 Series* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies the FindMe-FollowMe caller ID override for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#findme-followme**
(config-4444)**#findme-followme caller-id-override external number 2565551212**

first-name <*name*>

Use the **first-name** command to specify the user's first name. The name will represent the user's first name in the system. Use the **no** form of this command to remove a first name.

Syntax Description

<*name*>	Specifies the user's first name.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example specifies the first name of user **4444**:

(config)**#voice user 4444**
(config-4444)**#first-name John**

forward

Use the **forward** command to redirect all calls to this extension to a specified number. Forwarding calls allows the user to receive incoming calls at a different number. Use the **no** form of this command to disable this feature. Variations of this command include:

forward <*number*>
forward busy <*number*>
forward no-answer <*number*>

Syntax Description

<*number*>	Forwards all calls to the specified number. Do not include dashes or hyphens in the number.
busy <*number*>	Forwards calls to the specified number when the extension is busy. Do not include dashes or hyphens in the number.
no-answer <*number*>	Forwards unanswered calls to the specified number. Do not include dashes or hyphens in the number.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release R10.8.0	Command was expanded to include the **busy** and **no-answer** parameters.

Usage Examples

The following example forwards all calls to user **4444** to the number **256-555-8000**:

(config)**#voice user 4444**
(config-4444)**#forward 2565558000**

forward-disconnect

Use the **forward-disconnect** command to specify the method of manipulating the polarity to signal a disconnect of the line. Use the **no** form of this command to return to the default value. Variations of this command include:

forward-disconnect battery none
forward-disconnect battery remove
forward-disconnect battery reverse
forward-disconnect delay <*value*>

Syntax Description

battery none	Specifies that the battery will not be removed or reversed upon disconnect.
battery remove	Specifies that the battery will be removed upon disconnect.
battery reverse	Specifies that the battery will be reversed upon disconnect.
delay <*value*>	Sets a forward disconnect delay time value in milliseconds. Specify **250**, **500**, **750**, **1000**, or **2000** milliseconds.

Default Values

By default, **forward-disconnect battery remove** is enabled.

Command History

Release 9.3	Command was introduced.
Release A4.05	Command was expanded to include the **battery none** parameter.

Usage Examples

The following example removes the battery upon disconnect for user **4444**. This command is used most often with a fax machine that needs to be alerted that a call has ended:

(config)**#voice user 4444**
(config-4444)**#forward-disconnect battery remove**

fwd-courtesy

Use the **fwd-courtesy** command to enable the courtesy ring feature when a call is forwarded to notify the user that an incoming call has been re-routed. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sends a courtesy ring when a call is forwarded:

(config)**#voice user 4444**
(config-4444)**#fwd-courtesy**

group-ring-call-waiting

Use the **group-ring-call-waiting** command to enable the user to receive multiple calls from a ring group. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, users cannot receive multiple calls from a ring group.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example enables user **4444** to receive multiple calls from a ring group:

(config)**#voice user 4444**
(config-4444)**#group-ring-call-waiting**

hotel

Use the **hotel** command to allow extension reassignment to an alternate phone. Use the **no** form of this command to deny extension reassignment.

Syntax Description

No subcommands.

Default Values

By default, the hotel feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables the user to assign extension **4444** to an alternate phone:

(config)**#voice user 4444**
(config-4444)**#hotel**

hotline <*number*>

Use the **hotline** command to configure the user's phone as a hotline phone. When the user picks up the phone, it will automatically ring the extension assigned. Use the **no** form of this command to disable this feature.

Syntax Description

<*number*>	Specifies the hotline number to dial when the phone is off-hook.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets up user **4444** as a hotline and specifies that the number **256-555-8000** will be dialed when user 4444's phone is off-hook:

(config)**#voice user 4444**
(config-4444)**#hotline 2565558000**

last-name *<name>*

Use the **last-name** command to specify the user's last name. The stored name will appear in the caller ID information and directory for the user. Use the **no** form of this command to remove a last name.

Syntax Description

<name>	Specifies the user's last name.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example specifies the last name of user **4444**:

(config)**#voice user 4444**
(config-4444)**#last-name Smith**

location *<text>*

Use the **location** command to specify the user's physcial location within the company's physical address. The user's location is used to enhance emergency call email alert notification with the location of the caller. Use the **no** form of this command to remove the user's location.

Syntax Description

<text>	Specifies the user's location using no more than 40 characters.

Default Values

No default values are necessary for this command.

Command History

Release A4.03	Command was introduced.

Usage Examples

The following example specifies the location of user **4444**:

(config)**#voice user 4444**
(config-4444)**#location 5th floor, room 582**

message-waiting

Use the **message-waiting** command to configure message-waiting notification methods. Use this command to select the phone alert used to notify users of new voicemail. Use the **no** form of this command to disable this feature. Variations of this command include:

message-waiting both
message-waiting dialtone-only
message-waiting lamp-only

Syntax Description

both	Sets message-waiting notification for both dial tone and lamp.
dialtone-only	Sets message-waiting notification for dial tone only.
lamp-only	Sets message-waiting notification for lamp-only.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets message-waiting notification for user **4444** for both dial tone and lamp:

(config)**#voice user 4444**
(config-4444)**#message-waiting both**

modem-passthrough

Use the **modem-passthrough** command to switch to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings, such as echo cancellation and voice activity detection (VAD). Use the **no** form of this command to disable this feature. Variations of this command include:

modem-passthrough
modem-passthrough detection-time <*value*>
modem-passthrough cng-early-detect

Syntax Description

detection-time <*value*>	Optional. Specifies the fax and/or modem detection time length value in seconds. Range is **0** to **8** seconds.
cng-early-detect	Optional. Enables early (first burst) detection of fax calling (CNG) tone.

Default Values

By default, **modem-passthrough** is enabled.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command was expanded to include the **detection-time** parameter.
Release R10.8.0	Command was expanded to include the **cng-early-detect** parameter.

Usage Examples

The following example disables **modem-passthrough**:

(config)**#voice user 4444**
(config-4444)**#no modem-passthrough**

nls

Use the **nls** command to enable the non-linear suppression (NLS) option for the user. This option sets the echo canceller to reduce acoustic echo. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.

Usage Examples

The following example enables NLS for user **4444**:

```
(config)#voice user 4444
(config-4444)#nls
```

notify email

Use the **notify email** command to indicate either the primary or secondary email address for voicemail notification during the voicemail notification schedule. The primary and secondary email addresses must be configured using the commands *email <address> on page 4591* and *email-secondary <address> on page 4592*. Use the **no** form of this command to disable this feature. Variations of this command include the following:

notify email primary
notify email secondary

Syntax Description

primary	Specifies that email notifications for this schedule will be sent to the primary email address.
secondary	Specifies that email notifications for this schedule will be sent to the secondary email address.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was expanded.

Usage Examples

The following example configures the unit to send email notification for this schedule to the secondary email address.

(config)**#voice user 4444**
(config-4444)**#voicemail notify schedule monday 06:00 am**
Configuring New Schedule “monday 06:00 am”.
(config-4444-mon-06:00am)**#notify email secondary**

num-rings

Use the **num-rings** command to specify the number of rings for call pickup before the system redirects the call. Each system mode call coverage action can be configured with a different number of rings based on preference. Use the **no** form of this command to return to the default setting. Variations of this command include:

num-rings <*value*>
num-rings disabled
num-rings <*system mode*> <*value*>
num-rings <*system mode*> **disabled**
num-rings override <*value*>

Syntax Description

disabled	Optional. Specifies that the extension does not ring. This parameter is used when the FindMe-FollowMe feature is in call coverage mode and causes the FindMe-FollowMe actions to begin as soon as the incoming call is placed.
<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
override	Ignores the programmed system mode schedule.
<*value*>	Specifies the number of unanswered rings before the next call action begins. Specify **0** through **9** rings. Entering **0** specifies an unlimited number of rings.

Default Values

By default, the **num-rings** is set to **4**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was updated to include the system mode feature options.
Release A4.01	Command was expanded to include the **disabled** parameter.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

The **disabled** parameter specifies that the extension does not ring. This parameter is useful when the FindMe-FollowMe feature is enabled on the user account and is set as the preferred call coverage mode. For more information about configuring FindMe-FollowMe, refer to the *Configuring User Accounts on the NetVanta 7000 Series* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example allows the extension **4444** to ring **6** times before redirecting the call:

(config)**#voice user 4444**
(config-4444)**#num-rings 6**

The following example sets the number of rings to **1** before redirecting the call when the system mode is set to **weekend**:

(config)**#voice user 4444**
(config-4444)**#num-rings weekend 1**

The following example specifies that extension **4444** will not ring during lunch when the **lunch** system mode is enabled:

(config)**#voice user 4444**
(config-4444)**#num-rings lunch disabled**

password *<password>*

Use the **password** command to create a password or personal identification number (PIN) to protect voice settings and messages. Use the **no** form of this command to remove a password.

Syntax Description

<password>	Specifies a 4-digit password or PIN.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets the password for user **4444** to **4321**:

(config)#**voice user 4444**
(config-4444)#**password 4321**

plc

Use the **plc** command to enable packet loss concealment (PLC). PLC is used to prevent choppy connections by concealing a packet loss by replacing the lost packet with another voice packet in the data stream. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, PLC is enabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example disables PLC for user **4444**:

```
(config)#voice user 4444
(config-4444)#no plc
```

ppm queue reporting

Use the **ppm queue reporting** command to enable the viewing of call queue reporting statistics on the user's personal phone manager. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, users cannot view call queue reporting statistics from the personal phone manager.

Command History

Release R10.2.0	Command was introduced.

Usage Examples

The following example enables call queue reporting statistics are available to voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#ppm queue reporting**

remote-phone

Use the **remote-phone** command to specify using the source IPv4 address and port for routing rather than the Contact address specified in the SIP messaging. Enabling this feature also enables media anchoring for the voice user. Use the **no** form of this command to disable the settings.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example configures the voice user for extension **4444** as a remote phone:

(config)**#voice user 4444**
(config-4444)**#remote-phone**

rtp delay-mode

Use the **rtp delay-mode** command to configure the Realtime Transport Protocol (RTP) jitter buffer packet delay mode settings. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Use the **no** form of this command to return to the default setting. Variations of this command include:

rtp delay-mode adaptive
rtp delay-mode fixed

Syntax Description

adaptive	Configures RTP jitter buffer packet delay to adjust during a call based on network conditions.
fixed	Configures the RTP jitter buffer packet delay to remain constant.

Default Values

By default, the RTP delay mode is set to **adaptive**. This allows for minimal latency by adjusting the average packet delay based on the conditions of the network.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures RTP delay mode as f**ixed**:

(config)**#voice user 4444**
(config-4444)**#rtp delay-mode fixed**

rtp dtmf-relay

Use the **rtp dtmf-relay** command to configure the method by which Realtime Transport Protocol (RTP) dual tone multi-frequency (DTMF) events are relayed. The dial digits can be sent inband or out-of-band (OOB) of the voice stream. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp dtmf-relay inband
rtp dtmf-relay nte <*value*>

Syntax Description

inband	Specifies that RTP DTMF events be relayed inband in the RTP stream.
nte <*value*>	Specifies that RTP DTMF event value be relayed OOB using named telephone event (NTE). Enter an NTE value between **96** and **127**.

Default Values

By default, the **rtp dtmf-relay** is set for **NTE 101**.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example configures RTP DTMF relay events for **inband**:

(config)**#voice user 4444**
(config-4444)**#rtp dtmf-relay inband**

rtp dtmf-relay offer

Use the **rtp dtmf-relay offer** command to specify which dualtone multifrequency (DTMF) relay mode to offer to a particular Session Initiation Protocol (SIP) endpoint when using DTMF transcoding. Use the **no** form of this command to return the DTMF method to default value. Variations of this command include:

rtp dtmf-relay offer inband
rtp dtmf-relay offer nte <*value*>

Syntax Description

inband	Specifies that the DTMF relay method is in-band.
nte <*value*>	Specifies that the DTMF relay method is an RFC 2833 named telephone events (NTE). Valid NTE value range is **96** to **127**.

Default Values

By default, there is no preferred DTMF relay mode on the SIP endpoint, and the Session Border Controller (SBC) can choose a DTMF value that does not require transcoding to complete a call.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

The **rtp dtmf-relay offer** command is used to enable and configure DTMF transcoding on the AOS device when it is acting as an SBC. Transcoding is a method of translating media types in which the SBC operates as a translator for SIP devices using different media types that are attempting a connection. The AOS device translates one media type to another to allow the communication to succeed. For more information about transcoding and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

Before you can configure the DTMF relay method for transcoding, you must enable media anchoring using the command *ip rtp media-anchoring on page 1458*.

Usage Examples

The following example specifies the NTE 101 DTMF relay method for transcoding for voice user **4444**:

(config)**#ip rtp media-anchoring transcoding dtmf**
(config)**#voice user 4444**
(config-4444)**#rtp dtmf-relay offer nte 101**

rtp frame-packetization <*value*>

Use the **rtp frame-packetization** command to configure the Realtime Transport Protocol (RTP) frame packetization time in milliseconds for individual trunks and users. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP frame packetization time value in milliseconds. Select from **10**, **20**, **30**, or **40** milliseconds.

Default Values

By default, the **rtp frame-packetization** time is set to **20** milliseconds on all trunks and users.

Command History

Release 9.3	Command was introduced.
Release R10.8.0	Command was expanded to include **40** milliseconds.

Usage Examples

The following example sets the frame packetization time for user **4444** to **10** milliseconds:

(config)**#voice user 4444**
(config-4444)**#rtp frame-packetization 10**

rtp frame-packetization mode

Use the **rtp frame-packetization mode** command to specify the method for determining the Realtime Transport Protocol (RTP) frame packetization period on received calls. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp frame-packetization mode fixed
rtp frame-packetization mode negotiated

Syntax Description

fixed	Specifies that received calls always use the configured packetization period. This period is set using the command *rtp frame-packetization <value> on page 4617*.
negotiated	Specifies that the trunks and users use the packetization period specified in the Session Description Protocol (SDP) offer.

Default Values

By default, the **rtp frame-packetization mode** is set to **negotiated**.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example sets the method for determining the frame packetization mode for user **4444** to **fixed**:

(config)**#voice user 4444**
(config-4444)**#rtp frame-packetization mode fixed**

rtp media video filter

Use the **rtp media video filter** command to filter out video media attributes from transmitted or received Session Description Protocol (SDP) messages on an AOS device acting as a session border controller (SBC). You can filter out video media on a Session Initiation Protocol (SIP) endpoint by entering the command from the SIP endpoint's configuration mode. Use the **no** form of this command to disable the media filtering feature.

Syntax Description

No subcommands.

Default Values

By default, media filtering is disabled and all video SDP media attributes are passed through the SBC device.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

Media filtering is a part of the transcoding feature that is available when the AOS device is acting as an SBC. For more information about transcoding and the media filtering feature, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportofurms.adtran.com.

Usage Examples

The following example enables media filtering for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#rtp media video filter**

rtp packet-delay

Use the **rtp packet-delay** command to configure the maximum Realtime Transport Protocol (RTP) packet delays. This command is used to set the allowable limits of latency on the network. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp packet-delay fax <*value*>
rtp packet-delay maximum <*value*>
rtp packet-delay nominal <*value*>

Syntax Description

fax <*value*>	Sets the fax delay time value in milliseconds. Range is **0** to **500** milliseconds.
maximum <*value*>	Sets the maximum delay time value in increments of **10** milliseconds. Range is **40** to **320** milliseconds.
nominal <*value*>	Sets the nominal delay time value in increments of **10** milliseconds. Range is **10** to **240** milliseconds.

Default Values

By default, the RTP packet delay for fax is **300**, maximum is **100**, and nominal is **50**.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the RTP fax delay time for user **4444** to **200** milliseconds:

(config)**#voice user 4444**
(config-4444)**#rtp packet-delay fax 200**

rtp qos dscp <*value*>

Use the **rtp qos dscp** command to configure the maximum Realtime Transport Protocol (RTP) quality of service (QoS) parameters for differentiated services code point (DSCP). Use the **no** form of this command to return to the default global value.

Syntax Description

<*value*>	Configures the RTP QoS parameter for DSCP. Enter a value between **0** and **63**.

Default Values

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. The default global DSCP value for RTP is **46**.

Command History

Release 9.3	Command was introduced.

Functional Notes

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. QoS is set using a DSCP value. Valid DSCP values are **0** to **63**, and a higher DSCP value has a higher priority. The default global DSCP value for RTP is **46**. Remember that if you are using a public IP connection, such as the Internet, for Voice over Internet Protocol (VoIP), end-to-end QoS may not be guaranteed. The default DSCP value for Session Initiation Protocol (SIP) is **26**. To configure QoS for the RTP traffic that carries the voice conversation, use the command **ip rtp qos dscp** followed by the desired DSCP value.

Usage Examples

The following example configures the RTP QoS DSCP for user **4444** to **60**:

(config)**#voice user 4444**
(config-4444)**#rtp qos dscp 60**

script *<name>*

Use the **script** command to create a FindMe-FollowMe action script for the user and to enter the script's configuration mode. Use the **no** form of this command to remove the script from the user's FindMe-FollowMe configuration.

Syntax Description

<name>	Specifies the name of the action script using no more than **10** characters.

Default Values

By default, no FindMe-FollowMe action scripts are configured.

Command History

Release A4.01	Command was introduced.

Functional Notes

Each FindMe-FollowMe action script is the set of actions taken when FindMe-FollowMe is enabled and set as the call coverage mode for the user. Action scripts are associated with FindMe-FollowMe contact groups, and each group has one associated script. When the **script** command is entered from the user account's configuration mode, you will enter the action script configuration mode. Each action script can hold **10** actions.

For more information about enabling FindMe-FollowMe and specifying it as the call coverage mode for the user, refer to the commands *findme-followme on page 4593* and *coverage on page 4580*. For more information about contact group configuration, refer to *FindMe-FollowMe Contact Group Command Set on page 4752*. For more information about action script configuration, refer to *FindMe-FollowMe Action Script Command Set on page 4744*. For more information about configuring the FindMe-FollowMe feature, refer to the *Configuring User Accounts on the NetVanta 7000 Series* configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example creates the action script **BUSINESS** for user **4444**, and enters the script's configuration mode:

```
(config)#voice user 4444
(config-4444)#script BUSINESS
(config-4444-sc-BUSINESS)#
```


show voice mail

Use the **show voice mail** command to display a user's voicemail information. This command can also be executed from the Enable mode prompt using the syntax explained in *show voice mail on page 1081*. Variations of this command include:

show voice mail
show voice mail notify-schedule

> *The output of all **show** commands can be limited by appending the following modifiers to the end of the command: | **begin** <text>, | **exclude** <text>, and | **include** <text>. The **include** modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.*
>
> *For specific instructions and examples regarding these modifiers, refer to the introduction of the Enable Mode Command Set on page 94.*

Syntax Description

notify-schedule	Displays the voicemail notification schedule.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 17.1	Command was expanded to include the modifiers **begin**, **exclude**, and **include**.

Usage Examples

The following example shows sample output from the **show voice mail** command for extension **4444**:

```
(config)#voice user 4444
(config-4444)#show voice mail
Voicemail information for account: 4444
VM Class of Service: normal_voicemail
Standard Greeting (min): 01:00      Total Voicemail Usage (min): 05:00
Alternate Greeting (min): 01:00     Total Voicemail Free (min): 10:00
Recorded Name (min): 00:10
```


The following is sample output for the **show voice mail notify-schedule** command for extension **4444**:

(config)**#voice user 4444**
(config-4444)**#voicemail notify schedule monday 06:00 am**
Configuring New Schedule "monday 06:00 am".
(config-4444-mon-06:00am)**#show voice mail notify-schedule**

Start	End	Email 1	Email 2
Sun 12:00am	Sun11:59pm	---	---
Mon 12:00am	Mon5:59am	---	---
Mon 6:00am	at11:59pm	---	---

sip-authentication password *<password>*

Use the **sip-authentication password** command to configure the Session Initiation Protocol (SIP) authentication password for this user. Use the **no** form of this command to return the password to the default value.

Syntax Description

<password>	Specifies a string of up to 16 characters to be sent as the password in authentication.

Default Values

By default, the SIP authentication password is set to the same value as the currently configured SPRE PIN (typically **1234**) on all AOS devices except the NetVanta 7000 Series. By default, the SIP password for NetVanta 7000 Series products is a randomly generated 16 character password.

Command History

Release A2.04	Command was introduced.
Release R10.2.0	Command functionality was changed from using the SPRE password by default to being set to a randomly generated 16 character password by default for NetVanta 7000 Series products.

Usage Examples

The following example specifies that user **4444** will use the password **Password** for authentication:

(config)**#voice user 4444**
(config-4444)**#sip-authentication password Password**

The following example specifies that user **4444** on a NetVanta 7000 Series product will use a randomly generated 16 character password for authentication:

(config)**#voice user 4444**
(config-4444)**#no sip-authentication password**

sip-identity

Use the **sip-identity** command to configure the Session Initiation Protocol (SIP) registration options for the user. Use the **no** form of this command to disable the settings. Variations of this command include the following:

sip-identity <*station*> <*Txx*>
sip-identity <*station*> <*Txx*> **register**
sip-identity <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

<*station*>	Specifies the station to be used for SIP trunk (e.g., **station extension**).
<*Txx*>	Specifies the SIP trunk through which to register the server. The trunk is specified in the format Txx (e.g., **T01**).
register	Registers the user to the server.
auth-name <*username*>	Optional. Sets the user name that will be required as authentication for registration to the SIP server.
password <*password*>	Optional. Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example specifies trunk **T02** and extension **4400** for SIP **identity**:

(config)**#voice user 4444**
(config-4444)**#sip-identity 4400 T02**

sip-keep-alive

Use the **sip-keep-alive** command to configure the type of keep-alive method for this Session Initiation Protocol (SIP) trunk. Keep-alive messages must be sent between SIP device and the registrar to keep the connected channel open for communication. Use the **no** form of this command to return to disable this feature. Variations of this command include the following:

sip-keep-alive info
sip-keep-alive info <*value*>
sip-keep-alive options
sip-keep-alive options <*value*>

Syntax Description

info	Specifies the INFO method to be used for the keep-alives on the trunk.
options	Specifies the OPTIONS method to be used for the keep-alives on the trunk.
<*value*>	Optional. Specifies the amount of time in seconds between the type of SIP keep-alive messages being sent during a call. Range is **30** to **3600** seconds.

Default Values

By default, **sip-keep-alive** is set to **info 60** on NetVanta 7000 Series products. For IP business gateways (Total Access 900(e) Series and NetVanta 6000 Series) **sip-keep-alive** is disabled by default.

Command History

Release 13.1	Command was introduced
Release A2.04	Command was added to the Voice Line and Voice User command sets.

Usage Examples

The following example sets the keep-alive method to **info**:

(config)**#voice user 4444**
(config-4444)**#sip-keep-alive info**

sip-register send-unsynced

Use the **sip-register send-unsynced** command to disable the Session Initiation Protocol (SIP) synchronized registration method used for this voice user. When this command is enabled, AOS will register sip-identities regardless of whether the remote entity is registered. Use the **no** form of this command to use the synchronized registration method, in which SIP-identities will not be registered unless the remote entity is registered.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example specifies the use of synchronized registration for extension **4444**:

(config)**#voice user 4444**
(config-4444)**#no sip-register send-unsynced**

special-ring-cadences

Use the **special-ring-cadences** command to enable special ring cadences for this user. This command allows the user to be alerted with a distinctive ring. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example enables special ring cadences for user **4444**:

(config)**#voice user 4444**
(config-4444)**#special-ring-cadences**

speed-dial *<number>*

Use the **speed-dial** command to assign a number (1 through 20) to the user. The speed dial number allows the user to call each other by simply dialing 1- or 2-digit numbers. Use the **no** form of this command to disable this feature.

Syntax Description

<number>	Specifies the speed dial number for the user. Select from numbers **1** through **20**.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example assigns a **speed-dial** number to user **4444**:

(config)#**voice user 4444**
(config-4444)#**speed-dial 2**

station-lock

Use the **station-lock** command to lock the (station) against inbound or outbound calls. Locking a station will restrict phone privileges. Use the **no** form of this command to disable this feature. Variations of this command include:

station-lock admin
station-lock admin inbound
station-lock admin inbound-outbound
station-lock user
station-lock user inbound
station-lock user inbound-outbound

Syntax Description

admin	Allows the administrator to block calls.
user	Allows the user to block calls.
inbound	Optional. Blocks inbound calls.
inbound-outbound	Optional. Blocks both inbound and outbound calls.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example configures an administrator inbound and outbound station lock:

(config)**#voice user 4444**
(config-4444)**#station-lock admin inbound-outbound**

t38

Use the **t38** command to enable T.38 fax operation. Use the **no** form of this command to disable this feature.

The command modem-passthrough on page 4605 must be enabled for T.38 operation to work.

Syntax Description

No subcommands.

Default Values

By default, T.38 is disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables T.38 for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38**

Technology Review

T.38 is an International Telecommunication Union (ITU) specification that allows Group-3 Fax (T.30) data to be transported over the Internet. It is similar to dual tone multi-frequency (DTMF) relay (RFC 2833) in that the digital signal processor (DSP) decodes tones and demodulated fax data and converts them into packets. A similar device on the other end takes the packets/tones and remodulates them so that an analog fax machine on the other end can receive the fax. AOS's previous support (revisions 12 through 15) for fax/modem signals was simply detecting a tone and forcing the coder-decoder (CODEC) into G.711 and disabling/enabling echo cancellers based on the tones detected. When packet loss becomes high, sending faxes over G.711 becomes problematic, due to dropped messages and timeouts/retrains.

T.38 can be used in conjunction with various call-control schemes, such as H.323, Session Initiation Protocol (SIP), and Media Gateway Control Protocol (MGCP). AOS only supports SIP as the call-control method. This is typically referred to T.38/Annex-D. Annex-D describes the Session Initiation Protocol/Session Description Protocol (SIP/SDP) call establishment procedures.

t38 ced auto-generate

Use the **t38 ced auto-generate** command to specify when the digital signal processor (DSP) should regenerate the called station identifier (CED) signal toward the time division multiplexed (TDM) endpoint. If auto-generate is enabled, the DSP generates the CED signal only when it does not receive CED indicator packets from the Voice over IP (VoIP) endpoint. If auto-generate is disabled, the DSP generates the CED signal only when it does receive CED indicator packets from the VoIP endpoint. Using the **no** version of this command disables CED auto-generate.

Syntax Description

No subcommands.

Default Values

By default, CED auto-generate is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example enables CED auto-generate for the T.38 session for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 ced auto-generate**

t38 ced length <*time*>

Use the **t38 ced length** command to set the maximum duration of a regenerated called station identifier (CED) signal, in milliseconds, from the digital signal processor (DSP) toward the time division multiplexed (TDM) endpoint when a T.38 session is active. Using the **no** form of this command returns the duration to the default value.

Syntax Description

<time>	Specifies the maximum duration of a regenerated CED signal in milliseconds. Valid range is **0** to **4000** ms.

Default Values

By default, the maximum duration of a regenerated CED signal is **3000** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Setting the maximum duration of a regenerated CED signal to **0** effectively prevents any CED generation.

Usage Examples

The following example decreases the maximum duration of the CED signal to **2000** ms for the T.38 session for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 ced length 2000**

t38 cng-relay-selective

Use the **t38 cng-relay-selective** command to enable fax calling tones (CNG) relay only when V.21 messages are not being transmitted. Use the **no** version of this command to disable selective CNG relay.

Syntax Description

No subcommands.

Default Values

Selective CNG relay is disabled by default.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables T.38 CNG relay:

(config)**#voice user 4444**
(config-4444)**#t38 cng-relay-selective**

t38 ecm

Use the **t38 ecm** command to enable or disable error correction mode (ECM) during T.38 sessions. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 ecm enable
t38 ecm disable

Syntax Description

enable	Enables ECM during T.38 sessions.
disable	Disables ECM during T.38 sessions.

Default Values

By default, ECM is enabled.

Command History

Release R10.8.0	The command was introduced

Usage Examples

The following example disables ECM for T.38 sessions involving user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 ecm disable**

t38 error-correction

Use the **t38 error-correction** command to specify the type of fax error correction. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 error-correction fec
t38 error-correction redundancy

Syntax Description

fec	Specifies forward error correction (FEC) as the fax error correction. FEC is a system of error control where the sender adds redundant data to its messages, allowing the receiver to detect and correct errors (within certain bounds) without the need to request additional data from the sender.
redundancy	Specifies redundancy as the fax error correction. Redundancy error correction replicates the payload a user-specified number of times to determine if errors are present. The number of redundant packets is set using the command *t38 v21-preamble-timeout <value> on page 4644*).

Default Values

By default, **t38 error-correction** is set to **redundancy** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, the NetVanta 6240/6250 Serires, and the NetVanta 640 Series.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default value changed to **fec** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, and the NetVanta 7000 Series products.
Release R10.8.0	The default values for this command were updated.

Usage Examples

The following example sets the **t38 error-correction** to **fec** for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 error-correction fec**

t38 fallback-mode g711

Use the **t38 fallback-mode** command to specify the transmission mode used when T.38 fax relay cannot be successfully negotiated at the time of the fax transfer. Use the **no** form of this command to disable this feature.

Syntax Description

g711	Specifies that fax operation revert back to analog mode (G.711).

Default Values

By default, **t38 fallback-mode** is to **G.711**.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **G.711**.

Usage Examples

The following example enables the **t38 fallback-mode** for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 fallback-mode g711**

t38 generate-cng

Use the **t38 generate-cng** command to specify whether the digital signal processor (DSP) will begin a T.38 session by generating the calling signal (CNG) toward the time division multiplexed (TDM) endpoint. Using the **no** version of this command disables CNG generation.

Syntax Description

No subcommands.

Default Values

By default, CNG generation is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

With the introduction of this command, the CNG generation behavior of the T.38 session is now configurable. In AOS firmware prior to A5.01, this behavior was not configurable, but rather was set to always generate this signal.

Usage Examples

The following example enables CNG generation for the T.38 session for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 generate-cng**

t38 max-buffer <*value*>

Use the **t38 max-buffer** command to set the maximum buffer size for T.38 fax operation. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-buffer** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **800** bytes.

Default Values

By default, the maximum buffer size is set to **200**.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-buffer** to **100** for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 max-buffer 100**

t38 max-datagram <*value*>

Use the **t38 max-datagram** command to set the maximum datagram value in this unit. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-datagram** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **300** bytes.

Default Values

By default, the maximum datagram value is set to **72** bytes.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **72** bytes.

Usage Examples

The following example sets the **t38 max-datagram** to **100** for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 max-datagram 100**

t38 max-rate

Use the **t38 max-rate** command to specify the fax maximum rate. The actual transmission rate could be lower than specified rate if the receiving end cannot support the maximum rate. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 max-rate 14400
t38 max-rate 12000
t38 max-rate 2400
t38 max-rate 4800
t38 max-rate 7200
t38 max-rate 9600

Syntax Description

14400	Specifies 14400 bits per second (bps) as fax maximum rate.
12000	Specifies 12000 bps as fax maximum rate.
2400	Specifies 2400 bps as fax maximum rate.
4800	Specifies 4800 bps as fax maximum rate.
7200	Specifies 7200 bps as fax maximum rate.
9600	Specifies 9600 bps as fax maximum rate.

Default Values

By default, the maximum fax rate is set to **14400** bps.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-rate** to **4800** bps for user **4444**:

(config)#**voice user 4444**
(config-4444)#**t38 max-rate 4800**

t38 redundancy

Use the **t38 redundancy** command to set the number of redundant packets sent when the **t38 error-correction redundancy** feature is enabled. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 redundancy high-speed <*value*>
t38 redundancy low-speed <*value*>

Syntax Description

high-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for data messages (high-speed fax machine image data). Range is **0** (no redundancy) to **4** packets.
low-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for the signaling messages (low-speed fax machine protocol). Range is **0** (no redundancy) to **7** packets.

Default Values

By default, high-speed and low-speed redundancy values are set to **0** (no redundancy).

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables **t38 error-correction redundancy** and sets the number of redundant data messages to **3** for user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 error-correction redundancy**
(config-4444)**#t38 redundancy high-speed 3**

t38 v21-preamble-timeout *<value>*

Use the **t38 v21-preamble-timeout** command to set the maximum amount of time that the digital signal processor (DSP) waits for peer device activity after starting to transmit a V.21 preamble event before spoofing a response to the time division multiplexed (TDM) endpoint. Using the **no** version of this command returns the timeout value to the default setting.

Syntax Description

<value>	The time, in milliseconds, that the DSP will wait for peer activity. Valid range is **1** to **3000** ms.

Default Values

By default, the V.21 preamble timeout is set to **1700** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example specifies the V.21 preamble timeout value as **2000** ms for voice user **4444**:

(config)**#voice user 4444**
(config-4444)**#t38 v21-preamble-timeout 2000**

vad

Use the **vad** command to enable voice activity detection (VAD). VAD blocks out noise categorized as silence during a voice connection. The silent voice packets are not transmitted, allowing bandwidth usage to be reduced. Although VAD saves bandwidth, the quality of the voice call may be compromised. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, VAD is enabled for all voice trunks and users.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example disables VAD for user **4444**:

```
(config)#voice user 4444
(config-4444)#no vad
```

voicemail

Use the **voicemail** command to configure the voicemail options for the user. Use the **no** form of this command to disable the settings. Variations of this command include the following:

voicemail attachment-level <*dB*>
voicemail attachment-level disabled
voicemail auth-mode full
voicemail auth-mode none
voicemail auth-mode password
voicemail auto-play
voicemail cos <*name*>
voicemail delete-msg-on-email
voicemail envelope-play
voicemail greeting alternate
voicemail greeting default
voicemail greeting standard
voicemail language-preference English
voicemail language-preference FrenchCanadian
voicemail language-preference Irish
voicemail language-preference LatinAmSpanish
voicemail language-preference UKEnglish
voicemail new-user
voicemail notify email
voicemail notify email-secondary
voicemail notify email attach-message pcm
voicemail notify email attach-message pcm max-size <*size*>
voicemail notify email text-only
voicemail oper-assist <*number*>
voicemail password <*password*>

Syntax Description

attachment-level <*dB*>	Specifies the number of decibels for voicemail attachment files. Valid entries are **-30**, **-25**, **-20**, **-15**, or **-10** dB.
attachment-level disabled	Disables the automatic gain control (AGC) for voicemail attachments.
auth-mode	Specifies the authentication mode to access voicemail.
full	Specifies that the extension and password are required to access voicemail.
none	Specifies that voicemail authentication is disabled.
password	Specifies that the password is required to access voicemail. Only the password is required if set to password authentication mode.
auto-play	Specifies automatic playback of messages when entering the mailbox.
cos <*name*>	Configures the voicemail class of service (CoS) type by entering the name of the selected CoS.
delete-msg-on-email	Enables deletion of voicemail in email attachments.

envelope-play	Automatically plays message envelopes during message playback.
greeting	Specifies which greeting to use for voicemail.
alternate	Specifies using the alternate recorded voicemail greeting.
default	Specifies using the default voicemail greeting.
standard	Specifies using the user's standard recorded voicemail greeting.
language-preference	Specifies the language of the user's voicemail audio prompts.
English	Specifies English as the language of the user's voicemail audio prompts.
FrenchCanadian	Specifies French Canadian as the language of the user's voicemail audio prompts.
Irish	Specifies Irish as the language of the user's voicemail audio prompts.
LatinAmSpanish	Specifies Latin American Spanish as the language of the user's voicemail audio prompts.
UKEnglish	Specifies UK English as the language of the user's voicemail audio prompts.
new-user	Executes the new-user wizard for voicemail configuration.
notify email	Specifies sending an email notification when a new voicemail is received. This email is sent to the user's primary email address specified by the command *email <address> on page 4591*.
secondary	Specifies that the email notification is sent to the user's secondary email address. This address is specified by the command *email-secondary <address> on page 4592*.
attach-message	Sends the voicemail as a WAV file attachment to the specified email. The email client must be configured for email options to work.
pcm	Indicates that voicemail messages sent as email attachment will be in pulse-code modulation (PCM) format.
max-size <*size*>	Optional. Indicates truncating email attachments at the specified maximum size in kilobits (kb). Minimum size entry is **10** kb.
text-only	Sends only a text message to the specified email address.
oper-assist <*number*>	Directs all operator calls to the specified phone number.
password <*password*>	Creates the password/personal identification number (PIN) that will be required to access voicemail.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was expanded.
Release A2	Command was expanded to include the **notify email** parameters.
Release A2.04	Command was expanded to include **attachment-level** parameters.
Release A4.01	Command was expanded to include **auth-mode none** parameters.

Release A4.03	Command was expanded to include the **language-preference** parameter.
Release R10.2.0	Command was expanded to include the **Irish** language preference.
Release R10.5.0	Command was expanded to include the **UKEnglish** language preference.

Usage Examples

The following example sets the voicemail CoS for this user to **class1**:

(config)**#voice user 4444**
(config-4444)**#voicemail cos class1**

voicemail notify schedule

Use the **voicemail notify schedule** command to create a notification schedule for the user's voicemail message notification. When you create a notification schedule, you also enter the schedule's configuration mode. Using the **no** form of this command removes the notification schedule from the user's configuration. Variations of this command include:

voicemail notify schedule <*day*> <*HH:MM*> **am**
voicemail notify schedule <*day*> <*HH:MM*> **pm**

Once you have entered the **voicemail notify schedule** command, you are in the notification schedule configuration mode. From this mode you can enter the **notify email** command to specify whether notifications are sent to the primary or secondary user email address. Use the **no** form of this command to disable email notification. Variations of this command include:

notify email primary
notify email secondary

Syntax Description

<*day*>	Specifies the day of the week for the voicemail notification. Options include: **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, and **Sunday**.
<*HH:MM*>	Specifies the time of day voicemail notifications are sent in the HH:MM format. For example, to send a notification at **5:00**, enter **05:00**.
am	Specifies the voicemail notification time is in the a.m.
pm	Specifies the voicemail notification time is in the p.m.
primary	Specifies the email notification is sent to the user's primary email address. This address is specified using the command *email <address> on page 4591*.
secondary	Specifies the email notification is sent to the user's secondary email address. This address is specified using the command *email-secondary <address> on page 4592*.

Default Values

By default, no voicemail notification schedule is configured.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was expanded to include the secondary email address.

Usage Examples

The following example configures a voicemail notification schedule for user **4444**. This user is scheduled to receive voicemail notifications on **Monday** at **3:00 pm** by an email sent to the **primary** email address:

(config)**#voice user 4444**
(config-4444)**#voicemail notify schedule monday 03:00 pm**
Configuring New Schedule “monday 03:00 pm”.
(config-4444-mon-03:00pm)**#notify email primary**

warmline <*number*>

Use the **warmline** <*number*> command to configure the voice user to automatically call a specified phone number if an off-hook condition is detected, and a digit is not dialed within the specified time frame. Use the **no** version of this command to disable this feature. Variations of this command include:

warmline <*number*>
warmline <*number*> **delay** <*1-60*>

Syntax Description

<*number*>	Specifies a phone number to dial when an off-hook condition is detected.
delay <*1-60*>	Specifies the delay period to wait before dialing the warm line number. Valid range is **1** to **60** seconds.

Default Values

By default, there is no pre-provisioned warm line phone number. If a delay is not specified, the default delay is 20 seconds.

Command History

Release R11.10.0	Command was introduced.

Usage Examples

The following example configures a warm line phone number of **6002** using the default delay of **20** seconds for voice user **4444**:

(config)#**voice user 4444**
(config-4444)#**warmline 6002**

VOICE GROUPS COMMAND SETS

This section includes the following command sets:

VOICE CALL PICKUP GROUP COMMAND SET

Call pickup is a feature on AOS voice products that allows users to pick up calls ringing on other extensions without having to park calls. Call pickup works in two ways: either through directed call pickup, or call pickup groups. In directed call pickup, a user can answer the call dialing a special prefix (SPRE) code that includes the extension of the ringing phone. In call pickup groups, a group of users is created which allows calls to be answered by dialing the group extension. For example, to use the call pickup group, members of the group enter the four-digit extension of the call pickup group to answer a call. Ringing phones are identified either by hearing the phone ring or by monitoring the busy lamp field (BLF) on the IP phone. In a small office, for example, the receptionist might hear an employee's phone ringing. If the receptionist knows that employee is unable to answer, he or she can answer the call using the call pickup group. To do so, the receptionist dials **8509** (the extension of the call pickup group) and answers the call.

This section contains the commands necessary to create a call pickup group. A maximum of 10 call pickup groups can be created. For more information about the call pickup feature, refer to the *Configuring the Call Pickup Feature on AOS Voice Products* quick configuration guide available online at https://supportcommunity.adtran.com.

To create a call pickup group and enter the Call Pickup Group Configuration mode, enter the **voice pickup-group** at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice pickup-group Sales
Configuring New Pickup Group "Sales"
(config-Sales)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. for more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

member <extension> on page 4654
pickup-extension <extension> on page 4655

member <*extension*>

Use the **member** command to add members to the call pickup group. Use the **no** form of this command to remove the member from the group.

Syntax Description

<*extension*>	Specifies the four-digit extension of the user being added to the group.

Default Values

By default, no members are included in call pickup groups.

Command History

Release A4.01	Command was introduced.

Functional Notes

Use the **member** command as many times as necessary to add the desired number of members to the group.

Usage Examples

The following example adds the user with extension **1234** to the call pickup group **Sales**:

(config)**#voice pickup-group Sales**
(config-Sales)**#member 1234**

pickup-extension <*extension*>

Use the **pickup-extension** command to specify the extension dialed by members of the call pickup group to answer calls. To be used by the call pickup group, this extension must not be assigned to another user. Use the **no** form of this command to remove the extension from the call pickup group.

Syntax Description

<*extension*>	Specifies the four-digit extension used by members of the call pickup group to answer calls.

Default Values

By default, there is no pickup extension defined for call pickup groups.

Command History

Release A4.01	Command was introduced.

Functional Notes

The extension specified for the group must be a previously unassigned extension.

Usage Examples

The following example specifies that extension **8510** is used by the members of the call pickup group **Sales** to answer calls:

(config)**#voice pickup-group Sales**
(config-Sales)**#pickup-extension 8510**

VOICE ISDN GROUP COMMAND SET

Integrated services digital network (ISDN) groups are groups of ISDN trunks. Trunk groups combine one or more trunk accounts and assign outbound call characteristics to the grouped trunks. Individual trunk groups can be created for each trunk account. The trunk group is assigned outbound call capabilities (local calls, long distance calls, etc.). Additionally, a cost is assigned to each attribute in the outbound call template. For more information about configuring trunk groups in general, refer to the *NetVanta 7000 Series Trunk Accounts* configuration guide available online at https://supportcommunity.adtran.com.

In order to create a new ISDN group, you must first create the necessary ISDN trunks for your network. For more information on creating ISDN trunks, refer to the *Voice ISDN Trunk Command Set on page 5008*. There is also information on creating ISDN trunks in the *Total Access 900 Series ISDN PRI Interface* quick configuration guide available online at https://supportcommunity.adtran.com.

Once you have configured the necessary ISDN trunks, the ISDN trunk group is created by adding the trunk accounts to the ISDN group and defining the outbound call templates and costs. The commands for these procedures are covered in this command set.

To create an ISDN group and enter the ISDN Group Configuration mode, enter the **isdn-group** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#isdn-group 1
(config-isdn-group 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

call-type on page 4657
connect on page 4658
incoming-accept-number <number> on page 4659
max-channels <value> on page 4661
min-channels <value> on page 4662
resource pool-member <name> on page 4663

call-type

Use the **call-type** command to specify the type of communication allocated for this group. Use the **no** form of this command to return to the default value. Variations of this command include:

call-type analog
call-type any
call-type data
call-type voice

Syntax Description

analog	Configures the type of communication as 3.1 kHz audio.
any	Specifies that there are no restrictions on communication type.
data	Configures the type of communication as digital line.
voice	Configures the type of communication as speech.

Default Values

By default, the call type is set to **voice**.

Command History

Release 11.1	Command was introduced.
Release A4.03	Command was expanded to include **analog** call type.
Release R10.4.0	Command was expanded to include **any** and **data** call types.

Usage Examples

The following example sets the call type for integrated services digital network (ISDN) group **1** to **voice**:

(config)**#isdn-group 1**
(config-isdn-group 1)**#call-type voice**

connect

Use the **connect** command to associate a specific interface with the integrated services digital network (ISDN) group. Use the **no** form of this command to disconnect the specified interface from the ISDN group. Variations of this command include:

connect bri <*slot/port*>
connect pri <*interface id*>

Syntax Description

bri <*slot/port*>	Connects a basic rate interface (BRI) to the ISDN group. Slot and port number ranges are dependent upon the hardware installed in the unit. Type **connect bri ?** for information regarding valid ranges.
pri <*interface id*>	Connects a primary rate interface (PRI) to the ISDN group. Valid interface ID range is **1** to **255**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release R10.5.0	Command was expanded to include the BRI interface.

Usage Examples

The following example associates the **pri 1** interface with ISDN group **1**:

(config)**#isdn-group 1**
(config-isdn-group 1)**#connect pri 1**

incoming-accept-number <*number*>

Use the **incoming-accept-number** command to configure the incoming number to be accepted by this group from the public switched telephone network (PSTN). Use the **no** form of this command to remove a configured accept number.

Syntax Description

<*number*>	Specifies the phone number(s) accepted for this integrated services digital network (ISDN) group. The accept number entered should match the digits that populate the called party information element received on the ISDN interface for the call. Refer to the *Functional Notes* for more information on entering the number.

Default Values

By default, there are no configured incoming accept numbers. The ISDN group will not be able to accept calls without a configured incoming accept number.

Command History

Release 11.1	Command was introduced.

Functional Notes

Special characters (parentheses, commas, and dashes) can be entered in the incoming accept number for readability, but they are ignored by the system. Incoming accept numbers are entered as a single number, or as a range of numbers using the available wildcard characters.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

The following list provides some examples for proper wildcard usage:

Wildcard characters are especially useful in situations where ISDN hunt groups are deployed and the ISDN interfaces are all assigned to the same ISDN group in the router. ISDN hunt groups bundle multiple ISDN interfaces (with unique local directory numbers (LDNs)) together into a single group at the central office. When a call to any of the LDNs assigned to the ISDN interfaces in the hunt group is received at the central office, the switch sends the call to the first available ISDN interface. The ISDN group must be able to accept calls to multiple LDNs. Wildcard characters can simplify a configuration by allowing a single entry to match several numbers.

Usage Examples

The following example configures the group to accept calls for **256-555-1000** through **256-555-2000**:

(config)**#isdn-group 1**
(config-isdn-group 1)**#incoming-accept-number 256-555-[1,2]XXX**

max-channels <*value*>

Use the **max-channels** command to specify the maximum number of channels allocated for the integrated services digital network (ISDN) group. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the maximum number of channels allocated for the ISDN group. Valid range is from **1** to **255** channels.

Default Values

By default, the maximum number of channels is set to **0**. When **max-channels** is set to **0**, the group does not limit the number of usable channels and can use all available channels. Use the **no max-channels** command to return to the default value.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the maximum number of channels for ISDN group **1** to **50**:

(config)**#isdn-group 1**
(config-isdn-group 1)**#max-channels 50**

min-channels *<value>*

Use the **min-channels** command to specify the minimum number of channels allocated for the integrated services digital network (ISDN) group. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Specifies the minimum number of channels allocated for the ISDN group. Valid range is from **1** to **255** channels.

Default Values

By default, the minimum number of channels is set to **0**. When **min-channels** is set to **0**, no channels are reserved for this group. This group can use available channels, but does not have any channels specifically reserved. Use the **no min-channels** command to return to the default value.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the minimum number of channels for ISDN group **1** to **10**:

(config)**#isdn-group 1**
(config-isdn-group 1)**#min-channels 10**

resource pool-member <*name*>

Use the **resource pool-member** command to assign the group to a resource pool, making it a demand routing resource. Use the **no** form of this command to return to the default value.

Syntax Description

<*name*>	Specifies the name of the resource pool to which this group is assigned.

Default Values

By default, the group is not assigned to any resource pool.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the integrated services digital network (ISDN) group **1** as a member of resource pool **MyPool**:

(config)**#isdn-group 1**
(config-isdn-group 1)**#resource pool-member MyPool**

VOICE OPERATOR GROUP COMMAND SET

Voice operator groups are a subset of voice ring groups. Voice ring groups are groups of user accounts that can be called in a coordinated way with a single extension, and voice operator groups are one of these groups. Ring group members can log in when they want to receive calls from the group, and log out when they do not want to receive group calls.

Ring groups ring all members of the group simultaneously, and contain a single voice mailbox for the entire group. Operator groups can be configured to ring members by using a linear hunt method, in which calls are distributed to members in the order in which they were added to the group; by using uniform call distribution (UCD) method, in which calls are distributed to group members in the order in which they were added to the group in a uniform, round-robin fashion; and by using an all ring method, in which all members of the group are called and the first extension to pick up receives the call. Operator groups can also be configured to display operator calling-party identification.

Operator groups are always tied to extension zero, and calls from the operator group have a special ring cadence called a priority ring. A priority ring has two short rings, a long ring, and then silence. All other settings for the operator group are similar to those of normal ring groups.

For more information on voice operator groups and voice ring groups in general, refer to the *NetVanta 7000 Series Ring Groups and Operator Groups* quick configuration guide available online at https://supportcommunity.adtran.com, or to the *Voice Ring Group Command Set on page 4685*.

To enter the Voice Operator Group Configuration mode, enter the **voice operator-group** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice operator-group
(config-operator-group)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

coverage on page 4666
did <number> on page 4668
email <address> on page 4669
email-secondary <address> on page 4670

coverage

Use the **coverage** command to configure call coverage parameters for members of this group. The call coverage setting determines how a call is handled if the party dialed does not answer after a specified number of rings. Use the **no** form of this command to remove an individual coverage parameter. Variations of this command include:

coverage aa
coverage aa <*number*>
coverage internal <*number*>
coverage internal <*number*> **num-rings** <*value*>
coverage override aa
coverage override aa <*number*>
coverage override internal <*number*>
coverage override internal <*number*> **num-rings** <*value*>
coverage override vm
coverage override vm <*number*>
coverage vm
coverage vm <*number*>
coverage <*system mode*> **aa**
coverage <*system mode*> **aa** <*number*>
coverage <*system mode*> **internal** <*number*>
coverage <*system mode*> **internal** <*number*> **num-rings** <*value*>
coverage <*system mode*> **vm**
coverage <*system mode*> **vm** <*number*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to use for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
aa	Forwards the call to the default auto attendant.
aa <*number*>	Forwards the call to a specific extension programmed for the auto attendant. If no extension is specified, the phone is forwarded to the default auto attendant.
internal <*number*>	Forwards the call to the specified internal number.
num-rings <*value*>	Optional. Specifies the number of rings for the call before performing the next action. Valid range is **1** to **9**.
override	Ignores the programmed system mode schedule.
vm	Forwards the call to voicemail.
vm <*number*>	Optional. Forwards the call to the specified mailbox number.

Default Values

By default, no call coverage is specified.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was updated to include the voicemail and number of rings options.
Release 12.1	Command was updated to include the auto attendant options.
Release A1	Command was updated to include the system mode feature options.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

Usage Examples

The following example specifies that the call be forwarded to the internal extension **8500** after **3** rings.

(config)**#voice operator-group**
(config-operator-group)**#coverage internal 8500 num-rings 3**

did <*number*>

Use the **did** command to configure direct inward dialing (DID) for this group. DID is used if a service provider is providing digits to the unit on inbound calls or if the unit needs to provide DID information to a piece of customer premises equipment (CPE). Use the **no** form of this command to disable this feature.

Syntax Description

<*number*>	Defines the DID number assigned to the operator group.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example assigns DID **44** to the operator group:

(config)**#voice operator-group**
(config-operator-group)**#did 44**

email <*address*>

Use the **email** command to enter the email address for this operator group. Use the **no** form of this command to disable this feature.

Syntax Description

<*address*>	Specifies an email address for this group.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example creates an email contact for this group:

(config)**#voice operator-group**
(config-operator-group)**#email admin@helpdesk.com**

email-secondary *<address>*

Use the **email-secondary** command to enter a secondary email address for this operator group. Use the **no** form of this command to disable this feature.

Syntax Description

<address>	Specifies a contact email address for this group.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example creates a secondary email contact for this group:

(config)**#voice operator-group**
(config-operator-group)**#email-secondary lead@helpdesk.com**

login-member *<number>*

Use the **login-member** command to log an existing member of the operator group into the system. The **member** command must first be used to create a new group member. Use the **no** form of this command to disable this feature. Refer to *member <number> on page 4673* for more information.

Syntax Description

<number>	Specifies the extension number of the user who is logging in.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

This command allows a user to log in and out of an operator group, letting the system know when a user is available to accept calls.

Usage Examples

The following example logs in the user at extension **4422**:

(config)**#voice operator-group**
(config-operator-group)**#login-member 4422**

max-inbound <*value*>

Use the **max-inbound** command to define the maximum number of calls that can be inbound at the same time. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the maximum number of calls that can be inbound at the same time. Range is **1** to **10** calls.

Default Values

By default, the maximum number of inbound calls is set to **1**.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the maximum number of inbound calls to **3**:

(config)**#voice operator-group**
(config-operator-group)**#max-inbound 3**

member *<number>*

Use the **member** command to create a new member of the operator group. Use the **no** form of this command to remove a user's extension from an operator group.

Syntax Description

<number>	Specifies the extension number of the user to be added as an operator group member.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

A user can log in and out of the operator group using the **login-member** and **no login-member** commands. Refer to *login-member <number> on page 4671* for more information.

Usage Examples

The following example adds the user at extension **4422** to the operator group:

(config)**#voice operator-group**
(config-operator-group)**#member 4422**

num-rings <*value*>

Use the **num-rings** command to specify the number of rings for call pickup before the system redirects the call. Each system mode call coverage action can be configured with a different number of rings based on preference. Use the **no** form of this command to return to the default setting. Variations of this command include:

num-rings <*value*>
num-rings <*system mode*> <*value*>
num-rings override <*value*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
override	Ignores the programmed system mode schedule.
<*value*>	Specifies the number of rings before the next action. Specify **1** through **9** rings.

Default Values

By default, the maximum number of rings allowed at each extension is **2**.

Command History

Release 10.1	Command was introduced.
Release A1	Command was updated to include the system mode feature options.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

Usage Examples

The following example sets the maximum number of rings for the operator group to **6**:

(config)**#voice operator-group**
(config-operator-group)**#num-rings 6**

prefix

Use the **prefix** command to turn on the caller ID prefix for this ring group, causing **GRP:** to display in front of the caller ID information. Use the **no** form of this command to turn the prefix off. Variations of this command include:

prefix
prefix <*prefix*>

Syntax Description

<*prefix*>	Optional. Specifies an alphanumeric outbound calling name prefix. Maximum length is **40** characters.

Default Values

By default, no prefixes are enabled.

Command History

Release 10.1	Command was introduced.
Release A2.04	Command was expanded to include the optional <*prefix*> parameter.

Usage Examples

The following example turns on the caller ID prefix for the operator group:

(config)#**voice operator-group**
(config-operator-group)#**prefix**

sip-identity

Use the **sip-identity** command to configure the Session Initiation Protocol (SIP) registration options for the user. Use the **no** form of this command to disable the setting. Variations of this command include the following:

sip-identity <*station*> <*Txx*>
sip-identity <*station*> <*Txx*> **register**
sip-identity <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

<*station*>	Specifies the station to be used for SIP trunk (e.g., **station extension**).
<*Txx*>	Specifies the SIP trunk through which to register the server. The trunk is specified in the format Txx (e.g., **T01**).
register	Registers the user to the server.
auth-name <*username*>	Optional. Sets the user name that will be required as authentication for registration to the SIP server.
password <*password*>	Optional. Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 13.1	Command functionality was introduced to this section.

Usage Examples

The following example specifies trunk **T02** and extension **4400** for SIP identity:

(config)**#voice operator-group**
(config-operator-group)**#sip-identity 4400 t02**

type

Use the **type** command to configure the group type for the operator group. Variations of this command include:

type all
type executive
type linear
type ucd

Syntax Description

all	Configures the group as an all-inclusive operator group. When an operator group call comes in, all phones ring simultaneously.
executive	Configures an executive operator group. Refer to *email <address> on page 4692* for more information.
linear	Configures the group as a linear hunt operator group. Member phones ring one at a time until the call is picked up. When the next call comes in, the call cycle begins again by ringing the first operator group member. Refer to *member <number> on page 4673* for more information.
ucd	Configures the group as a uniform call distribution (UCD) operator group. Member phones ring one at a time until the call is picked up. When the next call comes in, the system remembers which member extension it last dialed and then continues the call cycle by ringing the next member in the operator group.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example configures all phones in the operator group to ring each time a call comes in:

(config)**#voice operator-group**
(config-operator-group)**#type all**

voicemail

Use the **voicemail** command to configure the voicemail options for the user. Use the **no** form of this command to disable the settings. Variations of this command include the following:

voicemail attachment-level <*dB*>
voicemail attachment-level disabled
voicemail auth-mode full
voicemail auth-mode password
voicemail auto-play
voicemail cos <*name*>
voicemail delete-msg-on-email
voicemail envelope-play
voicemail greeting alternate
voicemail greeting default
voicemail greeting standard
voicemail new-user
voicemail notify email attach-message pcm
voicemail notify email attach-message pcm max-size <*size*>
voicemail notify email text-only
voicemail oper-assist <*number*>
voicemail password <*password*>

Syntax Description

attachment-level <*dB*>	Specifies the number of decibels for voicemail attachment files. Valid entries are **-30**, **-25**, **-20**, -15, or **-10** dB.
attachment-level disabled	Disables the automatic gain control (AGC) for voicemail attachments.
auth-mode full	Specifies that the extension and password are required to access voicemail.
auth-mode password	Specifies that the password is required to access voicemail. Only the password is required if set to password authentication mode.
auto-play	Specifies automatic playback of messages when entering the mailbox.
cos <*name*>	Configures the voicemail class of service (CoS) type by entering the name of the selected CoS.
delete-msg-on-email	Enables deletion of stored voicemail on email attachments.
envelope-play	Automatically plays message envelopes during message playback.
greeting	Specifies which greeting to use for voicemail.
alternate	Specifies using the alternate recorded voicemail greeting.
default	Specifies using the default voicemail greeting.
standard	Specifies using the standard recorded voicemail greeting.
new-user	Executes the new-user wizard for voicemail configuration.
notify email	Specifies sending an email notification when a new voicemail is received.
attach-message	Sends the voicemail as a WAV file attachment to the specified email. The email client must be configured for email options to work.

pcm	Indicates message sent as email attachment will be in pulse-code modulation (PCM) format.
max-size <*size*>	Optional. Indicates truncating email attachments at the specified maximum size in kilobits (kb). Minimum size entry is **10** kb.
text-only	Sends only a text message to the specified email address.
oper-assist <*number*>	Directs all operator calls to the specified phone number.
password <*password*>	Creates the password/personal identification number (PIN) that will be required to access voicemail.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was expanded.
Release A2	Command was expanded to include the **notify email** parameters.
Release A2.04	Command was expanded to include **attachment-level** parameters.

Usage Examples

The following example sets the voicemail CoS to **class1**:

```
(config)#voice operator-group
(config-operator-group)#voicemail cos class1
```

VOICE PAGING GROUP COMMAND SET

The voice paging group configures handset paging parameters. Handset paging is a feature that provides paging to select groups of users through their IP phone handset. Handset paging works through a one-way audio transmission received as a call on individual IP phones, rather than on an overhead speaker using a private branch exchange (PBX) as overhead paging does. A handset page is initiated by a member of the paging group and sent to other members of the group. Voice paging groups are defined and organized using the commands in this section. For more information on using handset paging, refer to the *Handset Paging for the NetVanta 7000 Series* quick configuration guide available online at https://supportcommunity.adtran.com.

To activate the Voice Paging Group Configuration mode, enter the **voice paging-group** <*extension*> command from the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice paging-group 8956
  Configuring new paging group “8956”.
(config-8956)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

description <text> on page 80
do on page 81
end on page 82
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

codec on page 4681
include-paging-port on page 4682
member <extension> on page 4683
page-timeout <seconds> on page 4684

codec

Use the **codec** command to specify the coder-decoder (CODEC) that is used for the audio of the paging group. Use the **no** form of this command to return to the default. Variations of this command include:

codec g711alaw
codec g711ulaw
codec g722
codec g729

Syntax Description

g711alaw	Specifies the audio of the paging group is set to G.711 A-law 64 kilobits per second (Kbps).
g711ulaw	Specifies the audio of the paging group is set to G.711 U-law 64 Kbps.
g722	Specifies the audio of the paging group is set to G.722 8 Kbps.
g729	Specifies the audio of the paging group is set to G.729 8 Kbps.

Default Values

By default, the CODEC for the paging group is set to **G.729**.

Command History

Release A2.04	Command was introduced in the Voice Paging Group.

Functional Notes

The default CODEC used by paging groups is G.729, and is recommended for bandwidth optimization. Other CODECs can be used when a page initiator or recipient does not support G.729.

This **codec** command is not to be confused with the **codec** command used when creating CODEC lists (refer to *Voice CODEC List Command Set on page 4893* or *codec on page 4894*). This command does not create a list of CODECs, nor can it be entered multiple times. This **codec** command, used when configuring the voice paging group, specifies a single CODEC to be used by the paging group. If another CODEC is entered from the Voice Paging Group Configuration mode prompt, it will override any previous CODEC entries.

Usage Examples

The following example specifies the paging group using extension **8956** will use CODEC **G.722** for audio:

(config)**#voice paging-group 8956**
(config-8956)**#codec g722**

include-paging-port

Use the **include-paging-port** command to enable overhead paging for the paging group. Use the **no** form of this command to disable overhead paging for the paging group.

Syntax Description

No subcommands.

Default Values

By default, overhead paging is not enabled in paging groups.

Command History

Release A2.04	Command was introduced.

Functional Notes

Enabling the paging port for a handset paging group allows the page to transmit through IP phone handsets and an overhead paging system. This option will only function if an overhead paging system is available.

Usage Examples

The following example enables overhead paging for the paging group using extension **8956**:

(config)**#voice paging-group 8956**
(config-8956)**#include-paging-port**

member <*extension*>

Use the **member** command to add a new member to the paging group. Use the **no** form of this command to remove a member from the paging group.

Syntax Description

<*extension*>	Specifies the four-digit extension of the user to add to the paging group.

Default Values

By default, no members are included in a paging group.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example adds a user at extension **4567** to the paging group using extension **8956**:

(config)**#voice paging-group 8956**
(config-8956)**#member 4567**

page-timeout <*seconds*>

Use the **page-timeout** command to specify the amount of time page group users have to connect to the page before the call is started. Use the **no** form of this command to return to the default value.

Syntax Description

<*seconds*>	Specifies the time (in seconds) that users have to connect to a page before information is transmitted. Range is **1** to **10** seconds.

Default Values

By default, the page timeout is set to **2** seconds.

Command History

Release A2.04	Command was introduced.

Functional Notes

If no connection is made before the timeout period expires, the paging call is terminated.

Usage Examples

The following example sets the page timeout to **5** seconds for the paging group using extension **8956**:

(config)**#voice paging-group 8956**
(config-8956)**#page-timeout 5**

VOICE RING GROUP COMMAND SET

Voice ring groups define groups of user accounts that can be called in a coordinated way with a single extension. Ring group members can log in when they want to receive calls from the group, and log out when they do not want to receive group calls.

There are five ring group types to select from when creating a new ring group. The first of these types is a linear hunt group. In this type of group, calls are distributed to members in the order in which they were added to the ring group. The second type is the all ring group. In this type of group, all members of the group are called, and the first extension to answer receives the call. The third type is the uniform call distribution (UCD) group. In this group type, calls are distributed to members in the order in which they were added to the group, but in a uniform, round-robin fashion. The fourth type is an executive ring group. In this group type, calls are made to both the executive's and assistant's extensions, but the calls use the executive's call coverage. The last type is the operator ring group. This group type is detailed in the *Voice Operator Group Command Set on page 4664*.

Ring group's extensions must be unique and cannot begin with a **0** or a **9**. When configuring a new ring group, the extension defaults to one greater than the highest number ring group extension currently configured, or **8001** if no ring groups are configured. For more information about specific ring group configuration, refer to the *NetVanta 7000 Series Ring Groups and Operator Groups* quick configuration guide available online at https://supportcommunity.adtran.com.

To activate the Voice Ring Group Configuration mode, enter the **voice ring-group** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice ring-group xxxx*
(config-xxxx)#
```

*where xxxx = the ring group's four-digit extension.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

assistant-extension <*number*>

Use the **assistant-extension** command to tie an assistant's extension to an executive's extension.

*This command only applies to a ring group of **type executive**. Refer to type on page 4701 for more information.*

Syntax Description

<*number*>	Specifies the number of the assistant's extension.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

This command is used in conjunction with the **executive-extension** command (refer to *executive-extension <number> on page 4694*). When the executive's extension is dialed, both the assistant's and the executive's phones will ring. If neither phone is answered (or both are busy or set to do-not-disturb (DND)), the call is forwarded through the executive's call coverage list.

Usage Examples

The following example creates the executive ring group **1234** and causes both the executive (extension **4440**) and the assistant (extension **4444**) phones to ring when the executive extension is dialed:

(config)**#voice ring-group 1234**
(config-1234)**#type executive**
(config-1234)**#executive-extension 4440**
(config-1234)**#assistant-extension 4444**

cos

Use the **cos** command to set class of service (CoS) mode for the ring group. The CoS can be set to change for the members of the ring group based on the current system mode by including the system mode parameter. The CoS defines the types of phone service that will be available to the user during the time period. Use the **no** form of this command to disable this feature. Variations of this command include:

cos <*name*>
cos <*system mode*> <*name*>
cos no-access
cos <*system mode*> **no-access**
cos override <*name*>
cos override no-access

Syntax Description

<*name*>	Specifies the predefined CoS.
<*system mode*>	Optional. Specifies the system mode to configure. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
no-access	Blocks users from placing calls when applied to the CoS.
override	Ignores the programmed system mode schedule.

Default Values

By default, CoS is set to **no-access**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was expanded to include the system mode options.

Functional Notes

Additional functionality for this feature is provided by assigning a CoS to a specific system mode. When the system mode changes at a trigger point, the ring group's CoS changes.

For example, a CoS applied to the ring group when the system mode is specified as **night** can be used to prevent outbound calls during evening hours. System modes are defined from the Global Configuration mode using the command *voice system-mode on page 1971*.

Usage Examples

The following example assigns the CoS **Assistant** to the ring group **1234**:

(config)**#voice ring-group 1234**
(config-1234)**#cos Assistant**

coverage

Use the **coverage** command to configure call coverage parameters for members of this group. The call coverage setting determines how a call is handled if the party dialed does not answer after a specified number of rings. Use the **no** form of this command to remove an individual coverage parameter. Variations of this command include:

coverage aa
coverage aa <*number*>
coverage internal <*number*>
coverage internal <*number*> **num-rings** <*value*>
coverage operator
coverage operator num-rings <*value*>
coverage override aa
coverage override aa <*number*>
coverage override external <*number*>
coverage override internal <*number*>
coverage override internal <*number*> **num-rings** <*value*>
coverage override operator
coverage override operator num-rings <*value*>
coverage override vm
coverage override vm <*number*>
coverage vm
coverage vm <*number*>
coverage <*system mode*> **aa**
coverage <*system mode*> **aa** <*number*>
coverage <*system mode*> **external** <*number*>
coverage <*system mode*> **internal** <*number*>
coverage <*system mode*> **internal** <*number*> **num-rings** <*value*>
coverage <*system mode*> **operator**
coverage <*system mode*> **operator num-rings** <*value*>
coverage <*system mode*> **vm**
coverage <*system mode*> **vm** <*number*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
aa	Forwards the call to the default auto attendant.
aa <*number*>	Forwards the call to a specific extension programmed for the auto attendant. If no extension is specified, the phone is forwarded to the default auto attendant.
external <*number*>	Forwards the call to the specified external number. If no number is entered, the default auto answer is used.

internal <*number*>	Forwards the call to the specified internal number.
num-rings <*value*>	Optional. Specifies the number of rings for the call before performing the next action. Valid range is **1** to **9**.
operator	Forwards the call to the operator.
override	Ignores the programmed system mode schedule.
vm	Forwards the call to voicemail.
vm <*number*>	Optional. Forwards the phone to the specified mailbox number.

Default Values

By default, no call coverage is specified.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was updated to include the voicemail and number of rings options.
Release 12.1	Command was updated to include the auto attendant and operator options.
Release A1	Command was updated to include the system mode feature options.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

Usage Examples

The following example specifies that calls to the ring group **1234** be forwarded to the internal extension **8500** when in the **night** system mode.

(config)**#voice ring-group 1234**
(config-1234)**#coverage night internal 8500**

did <*number*>

Use the **did** command to configure direct inward dialing (DID) for this group. DID is used if a service provider is providing digits to the unit on inbound calls or if the unit needs to provide DID information to a piece of customer premises equipment (CPE). Use the **no** form of this command to disable this feature.

Syntax Description

<*number*>	Defines the DID number assigned to the ring group.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example assigns DID **44** to the ring group **1234**:

(config)**#voice ring-group 1234**
(config-1234)**#did 44**

email <*address*>

Use the **email** command to enter the email address for this user's group. Use the **no** form of this command to disable this feature.

Syntax Description

<*address*>	Specifies an email address for this group.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example creates an email contact for this group:

(config)**#voice ring-group 1234**
(config-1234)**#email admin@helpdesk.com**

email-secondary *<address>*

Use the **email-secondary** command to enter a secondary email address for this user's group. Use the **no** form of this command to disable this feature.

Syntax Description

<address>	Specifies a contact email address for this group.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example creates a secondary email contact for this group:

(config)**#voice ring-group 1234**
(config-1234)**#email-secondary lead@helpdesk.com**

executive-extension *<number>*

Use the **executive-extension** command to tie an executive's extension to an assistant's extension.

*This command only applies to **type executive** ring group(s). Refer to type on page 4701 for more information.*

Syntax Description

<number>	Specifies the number of the executive's extension.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

This command is used in conjunction with the **assistant-extension** command (refer to *assistant-extension <number> on page 4687*). When the executive's extension is dialed, both the assistant's and the executive's phones will ring. If neither phone is answered (or both are busy or set to do-not-disturb (DND)), the call is forwarded through the executive's call coverage list.

Usage Examples

The following example creates the executive ring group **1234** and causes both the executive (extension **4440**) and the assistant (extension **4444**) phones to ring when the executive extension is dialed:

(config)**#voice ring-group 1234**
(config-1234)**#type executive**
(config-1234)**#executive-extension 4440**
(config-1234)**#assistant-extension 4444**

login-member *<number>*

Use the **login-member** command to log an existing member of the ring group into the system. You must first use the member command to create a new group member. Use the **no** form of this command to disable this feature. Refer to *member <number> on page 4697* for more information.

Syntax Description

<number>	Specifies the extension number of the user who is logging in.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

This command allows a user to log in and out of a ring group, letting the system know when a user is available to accept calls.

Usage Examples

The following example logs in the user at extension **4422**:

(config)**#voice ring-group 1234**
(config-1234)**#login-member 4422**

max-inbound <*value*>

Use the **max-inbound** command to define the maximum number of calls that can be inbound at the same time. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the maximum number of calls that can be inbound at the same time. Range is **1** to **10** calls.

Default Values

By default, the maximum number of inbound calls is set to **1**.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the maximum number of inbound calls on ring group **1234** to **3**:

(config)**#voice ring-group 1234**
(config-1234)**#max-inbound 3**

member *<number>*

Use the **member** command to create a new member of the ring group. Use the **no** form of this command to remove a user's extension from a ring group.

Syntax Description

<number>	Specifies the extension number of the user you want to add as a ring group member.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

A user can log in and out of the ring group using the **login-member** and **no login-member** commands. Refer to *login-member <number> on page 4695* for more information.

Usage Examples

The following example adds the user at extension **4422** to the ring group **1234**:

(config)**#voice ring-group 1234**
(config-1234)**#member 4422**

num-rings

Use the **num-rings** command to specify the number of rings for call pickup before the system redirects the call. Each system mode call coverage action can be configured with a different number of rings based on preference. Use the **no** form of this command to return to the default setting. Variations of this command include:

num-rings <*value*>
num-rings <*system mode*> <*value*>
num-rings override <*value*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
override	Ignores the programmed system mode schedule.
<*value*>	Specifies the number of rings before the next action. Specify **0** through **9** rings. Entering **0** specifies an unlimited number of rings.

Default Values

By default, the **num-rings** is set to **4**.

Command History

Release 9.3	Command was introduced.
Release A1	Command was updated to include the system mode feature options.

Usage Examples

The following example sets the number of rings for this ring group to **6**:

(config)**#voice ring-group 1234**
(config-1234)**#num-rings 6**

prefix

Use the **prefix** command to turn on the caller ID prefix for this ring group, causing **GRP:** to display in front of the caller ID information. Use the **no** form of this command to turn the prefix off. Variations of this command include:

prefix
prefix <*prefix*>

Syntax Description

<*prefix*>	Optional. Specifies an alphanumeric outbound calling name prefix. Maximum length is **40** characters.

Default Values

By default, no prefixes are enabled.

Command History

Release 10.1	Command was introduced.
Release A2.04	Command was expanded to include the optional <*prefix*> parameter.

Usage Examples

The following example turns on the caller ID prefix for ring group **1234**:

(config)#**voice ring-group 1234**
(config-1234)#**prefix**

sip-identity

Use the **sip-identity** command to configure the Session Initiation Protocol (SIP) registration options for the user. Use the **no** form of this command to disable the settings. Variations of this command include the following:

sip-identity <*station*> <*Txx*>
sip-identity <*station*> <*Txx*> **register**
sip-identity <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

<*station*>	Specifies the station to be used for SIP trunk (e.g., **station extension**).
<*Txx*>	Specifies the SIP trunk through which to register the server. The trunk is specified in the format Txx (e.g., **T01**).
register	Registers the user to the server.
auth-name <*username*>	Optional. Sets the user name that will be required as authentication for registration to the SIP server.
password <*password*>	Optional. Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example specifies trunk **T02** and extension **4400** for SIP **identity**:

(config)**#voice ring-group 1234**
(config-1234)**#sip-identity 4400 T02**

type

Use the **type** command to configure the group type for the ring group. Variations of this command include:

type all
type executive
type linear
type ucd

Syntax Description

all	Configures the group as an all-inclusive ring group. When a ring group call comes in, all phones ring simultaneously.
executive	Configures an executive ring group. Refer to *executive-extension <number> on page 4694* for more information.
linear	Configures the group as a linear hunt ring group. Member phones ring one at a time until the call is picked up. When the next call comes in, the call cycle begins again by ringing the first ring group member. Refer to *member <number> on page 4697* for more information.
ucd	Configures the group as a uniform call distribution (UCD) ring group. Member phones ring one at a time until the call is picked up. When the next call comes in, the system remembers which member extension it last dialed and then continues the call cycle by ringing the next member in the ring group.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example configures the ring group **1234** to ring all phones in the ring group each time a call comes in:

(config)**#voice ring-group 1234**
(config-1234)**#type all**

voicemail

Use the **voicemail** command to configure the voicemail options for the user. Use the **no** form of this command to disable the settings. Variations of this command include the following:

voicemail attachment-level <*dB*>
voicemail attachment-level disabled
voicemail auth-mode full
voicemail auth-mode password
voicemail auto-play
voicemail cos <*name*>
voicemail delete-msg-on-email
voicemail envelope-play
voicemail greeting alternate
voicemail greeting default
voicemail greeting standard
voicemail new-user
voicemail notify email attach-message pcm
voicemail notify email attach-message pcm max-size <*size*>
voicemail notify email text-only
voicemail oper-assist <*number*>
voicemail password <*password*>

Syntax Description

attachment-level <*dB*>	Specifies the number of decibels for voicemail attachment files. Valid entries are **-30**, **-25**, **-20**, -15, or **-10** dB.
attachment-level disabled	Disables the automatic gain control (AGC) for voicemail attachments.
auth-mode full	Specifies that the extension and password are required to access voicemail.
auth-mode password	Specifies that the password is required to access voicemail. Only the password is required if set to password authentication mode.
auto-play	Specifies automatic playback of messages when entering the mailbox.
cos <*name*>	Configures the voicemail class of service (CoS) type by entering the name of the selected CoS.
delete-msg-on-email	Enables deletion of stored voicemail on email attachments.
envelope-play	Automatically plays message envelopes during message playback.
greeting	Specifies which greeting to use for voicemail.
alternate	Specifies using the alternate recorded voicemail greeting.
default	Specifies using the default voicemail greeting.
standard	Specifies using the standard recorded voicemail greeting.
new-user	Executes the new-user wizard for voicemail configuration.
notify email	Specifies sending an email notification when a new voicemail is received.
attach-message	Sends the voicemail as a WAV file attachment to the specified email. The email client must be configured for email options to work.

pcm	Indicates message sent as email attachment will be in pulse-code modulation (PCM) format.
max-size <*size*>	Optional. Indicates truncating email attachments at the specified maximum size in kilobits (kb). Minimum size entry is **10** kb.
text-only	Sends only a text message to the specified email address.
oper-assist <*number*>	Directs all operator calls to the specified phone number.
password <*password*>	Creates the password/personal identification number (PIN) that will be required to access voicemail.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was expanded.
Release A2	Command was expanded to include the **notify email** parameters.
Release A2.04	Command was expanded to include **attachment-level** parameters.

Usage Examples

The following example sets the voicemail CoS for this user to **class1**:

(config)**#voice ring-group 1234**
(config-1234)**#voicemail cos class1**

VOICE TRUNK GROUP COMMAND SET

Voice trunks are digital or analog subscriber lines delivered by service providers that allow communication devices to connect to the outside world. Voice trunk groups combine one or more trunk accounts and assign outbound call characteristics to the group. Individual trunk groups can be created for each trunk account. The trunk group is assigned outbound call capabilities (local calls, long distance calls, etc.). Additionally, a cost is assigned to each attribute in the outbound call template.

To create a trunk group, you must first configure individual trunk accounts. For more information on creating voice trunk accounts, refer to the following sections of this document:

- *Voice Analog Trunk Command Set on page 4959*
- *Voice SIP Trunk Command Set on page 5052*
- *Voice T1 Trunk Command Set on page 5151*

For more information about configuring trunk groups, refer to the *NetVanta 7000 Series Trunk Accounts* configuration guide available online at https://supportcommunity.adtran.com.

Integrated services digital network (ISDN) trunk groups are created using the command isdn-group <number> on page 1565. For more information regarding the creation of ISDN trunk groups, refer to the Voice ISDN Group Command Set on page 4656.

To enter the Voice Trunk Group Configuration mode, enter the **voice grouped-trunk** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice grouped-trunk TestGroup
(config-TestGroup)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

accept *<template>*

Use the **accept** command to specify numbers that users can dial on the trunk. This command controls the type of outbound calls users can place on the system. Use the **no** form of this command to remove a configured dial pattern and return to the default setting. Variations of this command include:

accept *<template>*
accept *<template>* **cost** *<value>*

Syntax Description

<template>	Specifies the patterns users can dial on the trunk. You can enter a complete phone number or wildcards can be used to help define accepted numbers. Refer to *Functional Notes* below for more information on using wildcards.
cost *<value>*	Specifies the cost value for the trunk. This option is used if a call is accepted by several trunks. The call will be routed to the trunk with the lowest cost value. The valid range is **0** to **499**.

Default Values

By default, the cost value is **zero**.

Command History

Release 9.3	Command was introduced.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example allows users on the trunk **TestGroup** to dial any local number:

(config)**#voice grouped-trunk TestGroup**
(config-TestGroup)**#accept Nxxxxxx**

deny

Use the **deny** command to add a proxy, automatic number identification (ANI) list, or trunk list to a voice trunk group's deny policy. Use the **no** form of this command to remove the proxy, ANI list, or trunk list from the deny policy. Variations of this command include:

deny list <*name*>
deny proxy

Syntax Description

list <*name*>	Specifies that either a trunk list or ANI list is added to the trunk group's deny policy.
proxy	Specifies that the proxy is added to the trunk group's deny policy.

Default Values

By default, no list or proxy is part of the trunk group's deny policy.

Command History

Release A2	Command was introduced.

Functional Notes

The trunk and ANI lists are created as part of the Source and ANI Based Routing (SABR) feature on AOS voice products. For more information about SABR, refer to the *SABR in AOS* configuration guide available online at https://supportcommunity.adtran.com. For more information about creating ANI or trunk lists, refer to *voice ani-list <name> on page 1891* or *voice trunk-list <name> on page 1979*.

Although there is no limit on the number of lists applied to voice trunk groups, it is important to remember that the more lists that are applied to a trunk group, the more the runtime performance of call routing will be affected.

Usage Examples

The following example applies the **TEST2** list to the deny policy of trunk group **TestGroup**:

(config)**#voice grouped-trunk TestGroup**
(config-TestGroup)**#deny list TEST2**

permit

Use the **permit** command to add a proxy, automatic number identification (ANI) list, or trunk list to a voice trunk group's permit policy. Use the **no** form of this command to remove the proxy, ANI list, or trunk list from the permit policy. Variations of this command include:

permit list <*name*>
permit proxy

Syntax Description

list <*name*>	Specifies that either a trunk list or ANI list is added to the trunk group's permit policy.
proxy	Specifies that the proxy is added to the trunk group's permit policy.

Default Values

By default, no list or proxy is part of the trunk group's permit policy.

Command History

Release A2	Command was introduced.

Functional Notes

The trunk and ANI lists are created as part of the Source and ANI Based Routing (SABR) feature on AOS voice products. For more information about SABR, refer to the *SABR in AOS* configuration guide available online at https://supportcommunity.adtran.com. For more information about creating ANI or trunk lists, refer to *voice ani-list <name> on page 1891* or *voice trunk-list <name> on page 1979*.

Although there is no limit on the number of lists applied to voice trunk groups, it is important to remember that the more lists that are applied to a trunk group, the more the runtime performance of call routing will be affected.

Usage Examples

The following example applies the **TEST1** list to the permit policy of trunk group **TestGroup**:

(config)**#voice grouped-trunk TestGroup**
(config-TestGroup)**#permit list TEST1**

reject *<template>*

Use the **reject** command to specify numbers users cannot dial on the trunk. This feature allows administrators to restrict callers from unwanted outbound calls, such as international calls and 900 numbers. Use the **no** form of this command to disable this feature.

Syntax Description

<template>	Specifies the patterns that users cannot dial on the trunk. You can enter a complete phone number or wildcards can be used to help define rejected numbers. Refer to *Functional Notes* below for more information on using wildcards. For example, you can enter **900$** to prevent users from dialing all 900 numbers.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.

2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.

3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].

4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example blocks calls to any 900 number on the trunk **TestGroup**:

(config)**#voice grouped-trunk TestGroup**
(config-TestGroup)**#reject 900$**

resource-selection

Use the **resource-selection** command to determine how the switchboard uses outbound call resources contained within a time division multiplexing (TDM) based trunk group. Use the **no** form of this command to disable this feature. Variations of this command include:

resource-selection circular
resource-selection circular ascending
resource-selection circular descending
resource-selection linear
resource-selection linear ascending
resource-selection linear descending

Syntax Description

circular	Performs call load balancing among available DS0s/B-channels in this trunk. Subsequent calls will be delivered to the next available DS0/B-channel in a round-robin fashion.
linear	Specifies that a call being delivered to this trunk will be accepted out the first available DS0/B-channel available at the time the call is received.
ascending	Optional. Distributes calls in an order from the lowest to the highest channel (DS0 1, 2, 3 through 24).
descending	Optional. Distributes calls in an order from the highest to the lowest channel (DS0 24, 23, 22 through 1).

Default Values

By default, resource selection is set to **linear**.

Command History

Release 9.3	Command was introduced.
Release 13.1	Command was expanded to include the ascending and descending subcommands.

Usage Examples

The following example specifies **circular** resource selection on the trunk **TestGroup**:

(config)**#voice grouped-trunk TestGroup**
(config-TestGroup)**#resource-selection circular**

trunk <*Txx*>

Use the **trunk** command to add an existing trunk to the trunk group so outbound calls may be placed out that particular trunk as well. Use the **no** form of this command to remove a configured trunk group.

Syntax Description

<*Txx*>	Specifies an ID number for the trunk. The trunk ID is in the format **Txx** where **xx** is the trunk ID number. Enter a trunk ID between **1** and **99**. For example, trunk **T02**.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example adds trunk **T02** to the trunk group **TestGroup**:

(config)**#voice grouped-trunk TestGroup**
(config-TestGroup)**#trunk t02**

VOICE SERVICES COMMAND SETS

This section includes the following command sets:

AUTO ATTENDANT COMMAND SET

Auto attendant is a voice feature that allows callers to be automatically transferred to an extension without any operator action. The commands in this section allow you to configure an auto attendant and to specify which files the auto attendant will use, as well as to configure Session Initiation Protocol (SIP) parameters so the auto attendant can be used in conjunction with system modes. For more information on configuring the voice auto attendant, refer to the *Configuring the Auto Attendant for NetVanta 7000 Series* configuration guide available online at https://supportcommunity.adtran.com.

To create an auto attendant and enter the Voice Auto Attendant Configuration mode, enter the **voice autoattendant** *<name> <extension>* command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice autoattendant Example 1212
(config-aa1212)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias "<text>" on page 75
cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

entry-filename <name> on page 4716
sip-identity on page 4717

entry-filename *<name>*

Use the **entry-filename** command to enter the extensible markup language (XML) file to use for this auto attendant. Use the **no** form of this command to disable the setting.

Syntax Description

<name>	Specifies the name of the XML file name to use for this auto attendant.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example shows the **entry-filename** command being executed to select the XML file to use for this auto attendant:

(config)**#voice autoattendant Example 1212**
(config-aa1212)**#entry-filename Operaa**

sip-identity

Use the **sip-identity** command to configure Session Initiation Protocol (SIP) registration options for the user. Use the **no** form of this command to disable the setting. Variations of this command include the following:

sip-identity <*station*> <*Txx*>
sip-identity <*station*> <*Txx*> **register**
sip-identity <*station*> <*Txx*> **register auth-name** <*username*> **password** <*password*>

Syntax Description

<*station*>	Specifies the station to be used for SIP trunk (e.g., **station extension**).
<*Txx*>	Specifies the SIP trunk through which to register the server. The trunk is specified in the format Txx (e.g., **T01**).
register	Registers the user to the server.
auth-name <*username*>	Sets the user name that will be required as authentication for registration to the SIP server.
password <*password*>	Sets the password that will be required as authentication for registration to the SIP server.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the auto attendant to use extension **5000** as its identity on trunk **T02**:

(config)**#voice autoattendant Example 1212**
(config-aa1212)**#sip-identity 5000 T02**

CALL COVERAGE COMMAND SET

The Call Coverage Command Set covers the commands used to configure the global call coverage list used on the AOS product. The call coverage list is used to control call routing when a voice user's phone is not answered. Call coverage can also be set on a per-user basis using the command *coverage on page 4580* from the user account configuration mode.

To create a global call coverage list and enter the list's configuration mode, enter the **voice coverage** command from the Global Configuration mode prompt as follows:

```
>enable
#configure terminal
(config)#voice coverage Evening
Configuring New Global Call Handling List "Evening".
(config-gch)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

coverage on page 4719
default on page 4721

coverage

Use the **coverage** command to configure global call coverage parameters for the AOS unit. The call coverage setting determines how a call is handled if the dialed party does not answer after a specified number of rings. Use the **no** form of this command to remove an individual coverage parameter. Variations of this command include:

coverage aa
coverage aa <*number*>
coverage internal <*number*>
coverage internal <*number*> **num-rings** <*value*>
coverage operator
coverage operator num-rings <*value*>
coverage override external <*number*>
coverage override global <*name*>
coverage override internal <*number*>
coverage override internal <*number*> **num-rings** <*value*>
coverage override operator
coverage override operator num-rings <*value*>
coverage override vm
coverage override vm <*number*>
coverage vm
coverage vm <*number*>
coverage <*system mode*> **aa**
coverage <*system mode*> **aa** <*number*>
coverage <*system mode*> **external** <*number*>
coverage <*system mode*> **internal** <*number*>
coverage <*system mode*> **internal** <*number*> **num-rings** <*value*>
coverage <*system mode*> **operator**
coverage <*system mode*> **operator num-rings** <*value*>
coverage <*system mode*> **vm**
coverage <*system mode*> **vm** <*number*>

Syntax Description

<*system mode*>	Optional. Specifies the system mode to configure for call coverage. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the *Functional Notes* of this command for more information on configuring system modes.
aa	Forwards the call to the default auto attendant.
aa <*number*>	Forwards the call to a specific extension programmed for the auto attendant. If no extension is specified, the phone is forwarded to the default auto attendant.
external <*number*>	Forwards the call to the specified external number. If no number is entered, the default auto answer is used.
internal <*number*>	Forwards the call to the specified internal number.

num-rings <*value*>	Optional. Specifies the number of rings for the call before performing the next action. Valid range is **1** to **9**.
operator	Forwards the call to the operator.
override	Ignores the programmed system mode schedule.
vm	Forwards the call to voicemail.
vm <*number*>	Optional. Forwards the phone to the specified mailbox number.

Default Values

By default, no system mode call coverage is specified.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was updated to include the voicemail and number of rings options.
Release 12.1	Command was updated to include the auto attendant, global, and operator options.
Release A1	Command was updated to include the system mode feature options.

Functional Notes

System mode call coverage provides more diverse functionality for call handling. In previous versions of AOS (revision 15.1 or earlier), up to five coverage modes were allowed. Calls were processed in the order in which the coverage options were entered into the system.

With the addition of the system mode options, up to five coverage options per system mode are allowed. The system modes can be modified using the command *voice system-mode on page 1971*.

Usage Examples

The following example specifies that the user's phone be forwarded to the internal extension **8500** when in the **night** system mode after **3** rings.

(config)**#voice coverage Evening**
(config-gch)**#coverage night internal 8500 num-rings 3**

default

Use the **default** command to specify the global call coverage list as the default list for the AOS unit. Use the **no** form of this command to remove the list as the default list.

Syntax Description

No subcommands.

Default Values

By default, no global call coverage list is configured.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example specifies that the global call coverage list **Evening** is the default coverage list and is used for all new users unless coverage is configured on a per-user basis:

```
(config)#voice coverage Evening
(config-gch)#default
```

CALL QUEUING COMMAND SET

Call queuing is a voice feature that pools multiple incoming calls into a single call queue that can be answered by members of the queue. The call queuing feature can be configured to play on-hold music and user-customized messages that inform callers of the status of their call.

For more information about configuring call queuing, refer to the quick configuration guide *Configuring Call Queuing on the NetVanta 7000 Series* available online at https://supportcommunity.adtran.com.

To create a call queue and enter the Voice Call Queuing Configuration mode, enter the **voice queue** <*extension*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice queue 6407
(config-6407)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

cross-connect on page 76
do on page 81
exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order:

call-distribution

Use the **call-distribution** command to specify the manner in which queued calls are distributed to members of the call queue. Use the **no** version of this command to restore the default.

Syntax Description

linear-hunt	Specifies that members of the call queue will be called in a linear, progressive fashion based on the foreign exchange service (fxs) port to which the queue member is connected.
most-idle-agent	Specifies that the member of the call queue who has not been on a call queue phone call for the longest duration of time will be called. Calls that end before the call queue greeting is played are not count as calls for the distribution list.
ring-all	Specifies that all members of the call queue will be called simultaneously.

Default Values

By default, all members of the call queue will be called simultaneously.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example configures the call-distrubtion as most-idle-agent:

(config)**# voice queue 6407**
(config-6407)**# call-distribution most-idle-agent**

deliver-member <*extension*>

Use the **deliver-member** command to send a call to a member extension even though that member is currently on the phone. Use the **no** version of this command to disable this feature.

Syntax Description

<*extension*>	Specifies the member extension.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sends a call to the member at extension **6535**:

(config)**# voice queue 6407**
(config-6407)**# deliver-member 6535**

dequeue-extension

Use the **dequeue-extension** command to set the dequeue extension for a call queue. People who are not members of the queue can call the dequeue extension to answer queued calls. Use the **no** version of this command to remove the dequeue extension.

Syntax Description

<*extension*>	Specifies the extension to be used as the dequeue extension.

Default Values

By default, no **dequeue-extension** is specified.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the dequeue extension of the call queue to **7900**:

(config)**# voice queue 6407**
(config-6407)**#dequeue-extension 7900**

description <*text*>

Use the **description** command to define a description for the call queue. Use the **no** version of this command to remove the description.

Syntax Description

<*text*>	Describes the call queue.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the call queue's description to **tech support queue**:

(config)**# voice queue 6407**
(config-6407)**#description tech support queue**

digit-action dial-extension <*extension*>

Use the **digit-action dial-extension** command to define the extension to which a queued caller will be forwarded if they press any digit on their phone while waiting in the queue. Use the **no** version of this command to disable this feature.

Syntax Description

<*extension*>	Specifies the extension to which callers will be forwarded.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the **digit-action dial-extension** for the call queue to **5150**:

(config)**# voice queue 6407**
(config-6407)**#digit-action dial-extension 5150**

greeting

Use the **greeting** command to configure all greeting types associated with the call queuing feature. Use the **no** version of this command to restore the system defaults.Variations of this command include:

greeting auto-page
greeting auto-page <*file*>
greeting auto-page extension <*extension*>
greeting auto-page immediate
greeting auto-page interval <*seconds*>
greeting periodic <*number*> <*file*>
greeting periodic <*number*> <*file*> **time** <*seconds*>
greeting pickup <*file*>
greeting welcome <*file*>

Syntax Description

<*file*>	Specifies the file name to be used as the greeting. If this file is not the default greeting file, it must be a G.729/G.711u/G.711a CODEC .wav file that was previously uploaded to the system by the system administrator using the **Audio Prompts** menu in the AOS graphical user interface (GUI).
auto-page	Specifies to page with a custom greeting plus a system generated prompt with the number of callers and the dequeue extension. The greeting will be followed by a system generated message saying **You have XX call(s) on YYYY**, where **XX** is the number of callers parked waiting in the queue and **YYYY** is the configured dequeue extension for this queue, or queue extension if the dequeue extension is not configured. If no <*file*> is specified for the greeting, the system precedes the system generated message with the call queue extension.
extension <*extension*>	Optional. Specifies a paging group extension from which to place the outgoing page. If no extension is specified, the message will go out over the overhead paging port.
immediate	Optional. Specifies to deliver a page immediately instead of waiting for the configured interval.
interval <*seconds*>	Optional. Specifies the number of seconds to wait to page after initiating the prior page. The valid range is **10** to **60** seconds.
periodic	Configures a call queue periodic greeting.
<*number*>	Specifies the index of the greeting to be configured.
time <*seconds*>	Optional. Specifies the number of seconds between periodic greetings. The valid range is **0** to **3600** seconds.
pickup	Configures a call queue pickup greeting.
welcome	Configures a call queue welcome greeting.

Default Values

By default, AOS uses system default periodic, pickup, and welcome greetings. The default settings for auto-page are **immediate** with an interval of **27** seconds.

Command History

Release A4.01	Command was introduced.
Release R10.10.0	Command was expanded to include the **auto-page** parameters. In addition, up to six queues are allowed.

Usage Examples

The following example sets the first periodic greeting for a call queue to **FILE1**:

(config)**# voice queue 6407**
(config-6407)**#greeting periodic 1 FILE1**

lock

Use the **lock** command to prevent new calls from entering the call queue. Use the **no** version of this command to unlock the call queue.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example locks the call queue:

(config)**# voice queue 6407**
(config-6407)**#lock**

login-member <*extension*>

Use the **login-member** command to log an existing queue member into the call queue. Use the **no** version of this command to log a member out of the call queue.

Syntax Description

<*extension*>	Specifies the extension of the call queue member.

Default Values

By default, members are logged out of the call queue.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example logs existing queue member **6535** into the call queue:

(config)**# voice queue 6407**
(config-6407)**# login-member 6535**

max-number-calls <*number*>

Use the **max-number-calls** command to define the maximum number of calls allowed in the call queue. Use the **no** version of this command to restore the system default.

Syntax Description

<*number*>	Specifies the maximum number of calls allowed in the call queue. The range for this command is dependent upon the NetVanta unit and will be reflected in an error message if the range is exceeded.

Default Values

By default, 16 calls are allowed in the call queue.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the maximum number of calls allowed in the queue to **10**:

(config)**# voice queue 6407**
(config-6407)**#max-number-calls 10**

max-wait-time <*seconds*>

Use the **max-wait-time** command to define the maximum amount of time a call can wait in the queue before being sent to the overflow extension. If no overflow extension is set, the call will remain in the queue until it is answered or the caller hangs up. Use the **no** version of this command to restore the default value.

Syntax Description

<*seconds*>	Indicates the maximum wait time in seconds, with a range from **30** to **6400**.

Default Values

By default, the **max-wait-time** is **3600** seconds.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the call queue's maximum wait time to **900** seconds:

(config)**# voice queue 6407**
(config-6407)**#max-wait-time 900**

member <*extension*>

Use the **member** command to add members to a call queue. Use the **no** version of this command to remove the member from the queue.

Syntax Description

<*extension*>	Specifies the extension of the member to be added.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example adds extension **6535** as a member of the call queue:

(config)**# voice queue 6407**
(config-6407)**#member 6535**

moh-external

Use the **moh-external** command to specify that a caller waiting for a call to be answered should hear music sourced from the external music on hold port (MOH). Use the **no** version of this command to return to the default setting. If external hold music is configured, the setting configured with the *lock on page 4731* will be ignored. The setting of the command *ringback-only on page 4742* overrides this setting.

Syntax Description

No subcommands.

Default Values

By default, the **moh-external** mode is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example specifies to use music on hold sourced from the MOH port for call queue extension **6407**:

(config)**# voice queue 6407**
(config-6407)**#moh-external**

moh-player <*name*>

Use the **moh-player** command to specify the name of the music on hold (MOH) player to use for queued callers. If the command *moh-external on page 4736* is configured, this setting will be ignored. The setting of the command *ringback-only on page 4742* overrides this setting. Use the **no** version of this command to return to the default setting.

Syntax Description

<*name*>	Specifies the name of the player.

Default Values

By default, the system's **default** MOH player, defined using the command *default on page 4854*, will be used if no player is specified for call queuing.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies the name of the MOH player used for call queue extension **6407** as **CQPLAYER**:

(config)**# voice queue 6407**
(config-6407)**#moh-player CQPLAYER**

name <*queue*>

Use the **name** command to define the name of a call queue. Use the **no** version of this command to remove the name of the queue.

Syntax Description

<*queue*>	Specifies the name of the call queue.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example defines the name of the call queue on extension **6407** as **TSQueue**:

(config)**# voice queue 6407**
(config-6407)**#name TSQueue**

overflow-extension <*extension*>

Use the **overflow-extension** command to define the extension to which a queued caller will be forwarded if the call queue is not available. This includes when the queue is locked, shutdown, at maximum capacity, or the call has been in queue past the maximum wait time. Use the **no** version of this command to remove the overflow extension.

Syntax Description

<*extension*>	Specifies the extension to which callers will be forwarded.

Default Values

By default, if no overflow extension is specified, queued calls will be dropped.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the overflow extension for the call queue to **5309**:

(config)**# voice queue 6407**
(config-6407)**#overflow-extension 5309**
(config-6407)#

prefix <*characters*>

Use the **prefix** command to define the characters that are pre-pended to calls coming into the call queue. The prefix is displayed along with the calling number in the call queue member's caller ID. Use the **no** version of this command to restore the system default.

Syntax Description

<*characters*>	Specifies the characters to be prepended to queued calls.

Default Values

By default, AOS pre-pends **CQ_** to all calls entering the call queue.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the prefix for the call queue to **TSQ**:

(config)**# voice queue 6407**
(config-6407)**#prefix TSQ**

rest-period <*seconds*>

Use the **rest-period** command to set the rest period for a call queue. The rest period is the amount of time after hanging up before another queued call can be sent to the member extension. Use the **no** version of this command to restore the system default.

Syntax Description

<*seconds*>	Specifies the length of the rest period, from **0** to **600** seconds.

Default Values

By default, the rest period is **120** seconds.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the call queue's rest period to **60** seconds:

(config)**# voice queue 6407**
(config-6407)**#rest-period 60**

ringback-only

Use the **ringback-only** command to set the call queue to ringback-only mode. Queued calls will hear only ringback instead of hold music and greetings, conserving system resources. Use the **no** version of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the ringback-only mode is disabled and the full-featured queue is available.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the call queue to ringback only mode:

(config)**# voice queue 6407**
(config-6407)**#ringback-only**

ring-time

Use the **ring-time** command to define the time (in seconds) that outbound calls from the call queue are allowed to ring logged-in members. Use the **no** version of this command to restore the system default.

Syntax Description

<seconds>	Specifies the ring-time, from **0** (unlimited) to **60** seconds..

Default Values

By default, the ring-time is **30** seconds.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the ring time for the call queue to **60** seconds:

(config)**# voice queue 6407**
(config-6407)**#ring-time 60**

FINDME-FOLLOWME ACTION SCRIPT COMMAND SET

FindMe-FollowMe is a feature supported by AOS that enables calls to be redirected based on who is calling and the availability of the called party. When the FindMe-FollowMe feature is enabled and configured, an incoming call rings the called party's extension for the amount of time specified by the number of rings, and then is redirected based on the configuration of the FindMe-FollowMe feature.

Configuring FindMe-FollowMe revolves around two main actions: configuring the user's contact group(s), and configuring the scripts used to determine which numbers are dialed in the FindMe-FollowMe call sequence. Contact groups are the groups of callers the user anticipates permitting to use the FindMe-FollowMe feature. For more information about configuring contact groups, refer to *FindMe-FollowMe Contact Group Command Set on page 4752*.

The second part of configuring FindMe-FollowMe is to specify the actions taken when an incoming call is received. The configurable actions include: calling the user extension, calling an internal extension, calling an external number, forwarding the call to an auto attendant, forwarding the call to voicemail, or sending an email to the called party. FindMe-FollowMe actions do not, however, include calling ring groups. Each of these actions that places a call can be configured for a specific timeout in which to stop the call, as well as prompt the called party for dual tone multi-frequency (DTMF) digits to manage the call. Each FindMe-FollowMe contact group can have **1** action script associated with it, and each script can have up to **10** actions, each of which can place up to **4** calls. Actions are numbered in the order you want them to be performed, but they can be entered in the command line interface (CLI) in any order. If you are working with actions in parallel, rather than sequence, configuring different ring times for different actions causes FindMe-FollowMe to delay the next action until the maximum ring time expires for the first action. This command set outlines the available commands for configuring FindMe-FollowMe action scripts.

For more information about configuring the FindMe-FollowMe feature, refer to the *Configuring User Accounts on the NetVanta 7000 Series* configuration guide available online at https://supportcommunity.adtran.com.

To create a FindMe-FollowMe action script for a voice user, enter the **script** command at the voice user configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice user 4444
(config-4444)#script Business
(config-4444-sc-Business)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81

All other commands for this command set are described in this section in alphabetical order.

action <*number*> email

Use the **action** <*number*> **email** command to specify that FindMe-FollowMe sends the called party an email notification of the call. Use the **no** form of this command to remove email notification from the action list. Variations of this command include:

action <*number*> **email primary**
action <*number*> **email secondary**

Syntax Description

<*number*>	Specifies the order number for the action. Valid range is **1** to **10**.
primary	Specifies that the email is sent to the user's primary email address.
secondary	Specifies that the email is sent to the user's secondary email address.

Default Values

By default, no action lists are configured.

Command History

Release A4.01	Command was introduced.

Functional Notes

This action sends an email to the called party's primary or secondary email address. These addresses are specified in the user account configuration mode using the commands *email <address> on page 4591* and *email-secondary <address> on page 4592*.

Usage Examples

The following example specifies that the **first** action for the action script **Business**, in user **4444**'s FindMe-FollowMe configuration, is to send a notification email to the user's **primary** email address:

(config)**#voice user 4444**
(config-4444)**#script Business**
(config-4444-sc-Business)**#action 1 email primary**

action <*number*> external <*phone number*>

Use the **action** <*number*> **external** command to specify that FindMe-FollowMe rings an external phone number to locate the called party. Use the **no** form of this command to remove this action from the action script. Variations of this command include:

action <*number*> **external** <*phone number*> **press-to-accept**
action <*number*> **external** <*phone number*> **press-to-accept ring-time** <*seconds*>
action <*number*> **external** <*phone number*> **no-press-to-accept**
action <*number*> **external** <*phone number*> **no press-to-accept ring-time** <*seconds*>

Syntax Description

<*number*>	Specifies the order number for the action. Valid range is **1** to **10**.
<*phone number*>	Specifies the external number to ring.
press-to-accept	Specifies that the called party is prompted to enter a digit to answer the call, generally selecting **1** to accept the call.
no-press-to-accept	Specifies that the called party is not prompted to enter a digit to answer the call.
ring-time <*seconds*>	Optional. Specifies the time (in seconds) that FindMe-FollowMe rings the external number before moving on to the next action in the list. Range is **1** to **60** seconds.

Default Values

By default, no external numbers are specified and the ring time is set to **24** seconds.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies that the first action for the action script **Business**, in user **4444**'s FindMe-FollowMe configuration, is to ring the external number of **12565550980**. For this action, the called party presses a digit to answer the call, and the ring time is specified at **30** seconds:

(config)**#voice user 4444**
(config-4444)**#script Business**
(config-4444-sc-Business)**#action 1 external 12565550980 press-to-accept ring-time 30**

action <*number*> internal <*extension*>

Use the **action** <*number*> **internal** command to specify that FindMe-FollowMe rings an internal extension to locate the called party. Use the **no** form of this command to remove this action from the action script. Variations of this command include:

action <*number*> **internal** <*extension*> **press-to-accept**
action <*number*> **internal** <*extension*> **press-to-accept ring-time** <*seconds*>
action <*number*> **internal** <*extension*> **no-press-to-accept**
action <*number*> **internal** <*extension*> **no-press-to-accept ring-time** <*seconds*>

Syntax Description

<*number*>	Specifies the order number for the action. Valid range is **1** to **10**.
<*extension*>	Specifies the internal extension to ring.
press-to-accept	Specifies that the called party is prompted to enter a digit to answer the call, generally selecting **1** to accept the call.
no-press-to-accept	Specifies that the called party is not prompted to enter a digit to answer the call.
ring-time <*seconds*>	Optional. Specifies the time (in seconds) that FindMe-FollowMe rings the external number before moving on to the next action in the list. Range is **1** to **60** seconds.

Default Values

By default, no internal numbers are specified and the ring time is set to **24** seconds.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies that the first action for the action script **Business**, in user **4444**'s FindMe-FollowMe configuration, is to ring the internal extension of **8989**. For this action, the called party presses a digit to answer the call, and the ring time is specified at **30** seconds:

(config)**#voice user 4444**
(config-4444)**#script Business**
(config-4444-sc-Business)**#action 1 internal 8989 press-to-accept ring-time 30**

action <*number*> refer <*extension*>

Use the **action** <*number*> **refer** command to specify that FindMe-FollowMe refers an incoming call to another user. Use the **no** form of this command to remove the action from the action script.

Syntax Description

<*number*>	Specifies the order number for the action. Valid range is **1** to **10**.
<*extension*>	Specifies the user extension to which the call is referred.

Default Values

By default, no action scripts are configured.

Command History

Release A4.01	Command was introduced.

Functional Notes

When a **refer** action is added to the action script, no other actions are performed after the **refer**. When a FindMe-FollowMe call is referred to another user, the call no longer uses the FindMe-FollowMe action script, but rather uses the call coverage configured for the user to which the call was referred.

Usage Examples

The following example specifies that the fifth and final action for the action script **Business**, in user **4444**'s FindMe-FollowMe configuration, is to refer the call to user **1234**. When the call is accepted by extension **1234**, the call follows the call coverage configured for that user.

(config)**#voice user 4444**
(config-4444)**#script Business**
(config-4444-sc-Business)**#action 5 refer 1234**

action <*number*> vm

Use the **action** <*number*> **vm** command to specify that FindMe-FollowMe sends the caller to voicemail. Use the **no** form of this command to remove the action from the action script. Variations of this command include:

action <*number*> **vm**
action <*number*> **vm** <*mailbox*>

Syntax Description

<*number*>	Specifies the order number for the action. Valid range is **1** to **10**.
<*mailbox*>	Optional. Sends the caller to a specific voice mailbox, rather than the user's mailbox.

Default Values

By default, the call is sent to the user's voice mailbox unless another mailbox is specified.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies that the fourth action for the action script **Business**, in user **4444**'s FindMe-FollowMe configuration, is to send the call to the user's voice mailbox:

(config)**#voice user 4444**
(config-4444)**#script Business**
(config-4444-sc-Business)**#action 4 vm**

description *<"text">*

Use the **description** command to enter a short description of the action script. This description can be useful when you have multiple scripts and contact groups configured. Use the **no** form of this command to remove the description.

Syntax Description

<"text">	Describes the action script. The text should be enclosed in quotation marks.

Default Values

By default, no action scripts are configured.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example creates a description (**New Business Contacts**) for the action script **Business** (in user **4444**'s FindMe-FollowMe configuration):

(config)**#voice user 4444**
(config-4444)**#script Business**
(config-4444-sc-Business)**#description "New Business Contacts"**

FINDME-FOLLOWME CONTACT GROUP COMMAND SET

FindMe-FollowMe is a feature supported by AOS that enable calls to be redirected based on who is calling. When the FindMe-FollowMe feature is enabled and configured, an incoming call rings the called party's extension for a specified number of rings, and then is redirected based on the configuration of the FindMe-FollowMe feature.

Configuring FindMe-FollowMe revolves around two main actions: configuring the user's contact group(s), and configuring the scripts used to determine which numbers are dialed in the FindMe-FollowMe sequence. Contact groups are the groups of callers the user anticipates permitting to use the FindMe-FollowMe feature. For example, a user might have a contact group for family and one for business partners. New contact groups can be added or removed at any time, and each user can have up to **5** contact groups. In addition, contact groups can be configured to play a courtesy greeting, prompt the caller for their name, enable callers to leave a voicemail, provide ringback to the inbound caller, and add or remove group members based on their calling number. This command set outlines the available commands for configuring FindMe-FollowMe contact groups.

For more information about configuring action scripts, refer to *FindMe-FollowMe Action Script Command Set on page 4744*. For more information about configuring the FindMe-FollowMe feature, refer to the *Configuring User Accounts on the NetVanta 7000 Series* configuration guide available online at https://supportcommunity.adtran.com.

To create a FindMe-FollowMe contact group for a voice user, enter the **contact-group** command at the voice user configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice user 4444
(config-4444)#contact-group 1
(config-4444-cg-1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81

All other commands for this command set are described in this section in alphabetical order.

ringback on page 4761

courtesy-greeting

Use the **courtesy-greeting** command to enable a courtesy greeting for the inbound caller while FindMe-FollowMe performs actions to locate the called party. The courtesy greeting provided by AOS tells callers to "Please wait while I locate your party." Using the **no** form of this command disables the courtesy greeting.

Syntax Description

No subcommands.

Default Values

By default, the courtesy greeting is enabled.

Command History

Release A4.01	Command was introduced.

Functional Notes

If ringback is enabled in the FindMe-FollowMe contact group, then all prompts and greetings are ignored.

Usage Examples

The following example disables the courtesy greeting for contact group **2** in voice user **4444**'s FindMe-FollowMe configuration:

(config)**#voice user 4444**
(config-4444)**#contact-group 2**
(config-4444-cg-2)**#no courtesy-greeting**

digit-prompt

Use the **digit-prompt** command to enable dual tone multi-frequency (DTMF) digit prompting for the FindMe-FollowMe contact group. When DTMF digit prompting is enabled, inbound callers can control the incoming call using DTMF tones. When callers hear the prompt "To leave a voicemail at any time, press 1," they can then press 1 to leave a voicemail message. Using the **no** form of this command disables DTMF digit prompting for the contact group.

Syntax Description

No subcommands.

Default Values

By default, DTMF digit prompting is disabled in FindMe-FollowMe.

Command History

Release A4.01	Command was introduced.

Functional Notes

To use DTMF digit prompting, enhanced FindMe-FollowMe must be enabled on the user account. Refer to the command *findme-followme on page 4593* for more information.

Usage Examples

The following example enables DTMF digit prompting for contact group **2** in voice user **4444**'s FindMe-FollowMe configuration:

```
(config)#voice user 4444
(config-4444)#contact-group 2
(config-4444-cg-2)#digit-prompt
```


group-description *<"text">*

Use the **group-description** command to enter a short description for the contact group. Using the **no** form of this command removes the group description.

Syntax Description

<"text">	Describes the contact group. Enter the descriptions in quotation marks.

Default Values

By default, no group description exists.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example describes contact group **2** in voice user **4444**'s FindMe-FollowMe configuration as **Business Contacts**:

(config)**#voice user 4444**
(config-4444)**#contact-group 2**
(config-4444-cg-2)**#group-description "Business Contacts"**

implicitly-allow

Use the **implicitly-allow** command to specify the callers that are implicitly allowed into the user's FindMe-FollowMe contact group. Using the **no** form of this command removes implicit users from the contact group. Variations of this command include:

implicitly-allow all
implicitly-allow external
implicitly-allow internal

Syntax Description

all	Specifies that all callers are implicitly included in the contact group.
external	Specifies that only external callers are implicitly included in the contact group.
internal	Specifies that only internal callers are implicitly included in the contact group.

Default Values

By default, no users are included implicitly in a contact group.

Command History

Release A4.01	Command was introduced.

Usage Examples

In the following example, **external** callers are implicitly included in contact group **2** for voice user **4444**'s FindMe-FollowMe configuration:

(config)**#voice user 4444**
(config-4444)**#contact-group 2**
(config-4444-cg-2)**#implicitly-allow external**

permit-caller-id number <*number*>

Use the **permit-caller-id number** command to add explicitly known numbers to the contact group and make them members of the group. Using the **no** form of this command removes the member from the group. Variations of this command include:

permit-caller-id number <*number*>
permit-caller-id number <*number*> <*"description"*>

Syntax Description

<*number*>	Specifies the calling number of the known member to add to the contact group.
<*"description"*>	Optional. Specifies a short description of the member to add to the group. Descriptions should be in quotation marks.

Default Values

By default, no members are explicitly included in the contact group.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example adds the member **Company A VIP** (who calls from number **12565557890**) to contact group **2** of voice user **4444**'s FindMe-FollowMe configuration:

(config)#**voice user 4444**
(config-4444)#**contact-group 2**
(config-4444-cg-2)#**permit-caller-id number 12565557890 "Company A VIP"**

presence available script <*name*>

Use the **presence available script** command to associate previously configured action scripts with a user's FindMe-FollowMe contact group. Using the **no** form of this command removes the script from the contact group.

Syntax Description

<*name*>	Specifies which action script is associated with the contact group.

Default Values

By default, no action scripts are associated with the contact group.

Command History

Release A4.01	Command was introduced.

Functional Notes

FindMe-FollowMe works by executing actions to locate the called party. These actions are determined by configuring action scripts for each contact group. Each contact group can have **1** action script associated with it, and each action script can support up to **10** actions. For more information about configuring FindMe-FollowMe action scripts, refer to *FindMe-FollowMe Action Script Command Set on page 4744*.

Usage Examples

In the following example, the action script **Business** is associated with contact group **2** in voice user **4444**'s FindMe-FollowMe configuration:

(config)**#voice user 4444**
(config-4444)**#contact-group 2**
(config-4444-cg-2)**#presence available script Business**

record-calling-name

Use the **record-calling-name** command to enable a prompt that asks incoming callers to record their names. When the name recording option is enabled, the system records **3** seconds of audio before moving on to other scripts or actions. Using the **no** form of this command disables the name recording feature.

Syntax Description

No subcommands.

Default Values

By default, callers are not prompted to record their names.

Command History

Release A4.01	Command was introduced.

Functional Notes

When ringback is enabled for the contact group, all prompts and greetings are ignored.

Usage Examples

The following example enables caller name recording in contact group **2** of voice user **4444**'s FindMe-FollowMe configuration:

(config)**#voice user 4444**
(config-4444)**#contact-group 2**
(config-4444-cg-2)**#record-calling-name**

ringback

Use the **ringback** command to enable ringback for the contact group. When ringback is enabled, inbound FindMe-FollowMe calls are only answered when an outbound call is answered or if one of the FindMe-FollowMe actions requires the call to be answered (for example, voicemail). If ringback is disabled, then the call is answered immediately, any configured greetings are played, and music on hold is eventually played while the called party is located. Using the **no** form of this command disables ringback.

Syntax Description

No subcommands.

Default Values

By default, ringback is disabled.

Command History

Release A4.01	Command was introduced.

Functional Notes

Ringback must be disabled for any contact group configured prompts or greetings to be played. However, using the prompts and greetings can drain system resources. Adtran recommends you use ringback as much as possible to save these resources.

Usage Examples

The following example enables ringback for contact group **2** in voice user **4444**'s FindMe-FollowMe configuration:

(config)**#voice user 4444**
(config-4444)**#contact-group 2**
(config-4444-cg-2)**#ringback**

HMR COMMAND SET

Header manipulation rules (HMR) manipulation is a feature used in AOS that allows the manipulation of both headers and message bodies in Session Initiation Protocol (SIP) transmissions, based on configurable rules. These rules can be applied to both outbound and inbound messages, and can be used to modify existing headers or the body of SIP messages, match, add, or remove SIP headers, and store variable information. In addition, message manipulation rules can use regular expressions to modify SIP headers and message bodies. One of the benefits of using SIP header and message manipulation is that the feature can give you enhanced control over the behavior of SIP traffic on your AOS device, as well as help solve interoperability issues between the AOS device and other products.

SIP header manipulation is achieved by creating an HMR policy, a set of HMR rules, and applying those rules to the HMR policy. The policy is then applied to a SIP trunk, to all SIP traffic in the AOS device, to SIP traffic sent or received by a SIP proxy user, or to SIP traffic sent or received by a SIP proxy server. The HMR policies can be applied to either inbound or outbound SIP traffic. In addition, HMR variables can be created, which store text used in header manipulation. These variables can be public or private, indicating their scope of access, or Call-ID variables. Public variables are accessible and shared by all HMR policies. Private variables exist within an instance of a policy. Call-ID variables are similar to public variables, in that they are available to all policies, but their value is limited in scope to the current Call-ID. In addition, system variables can be used to provide predefined variables (such as public, private, or Call-ID variables) access to system-level information.

The following are the basic configuration steps needed to create SIP header manipulation in AOS:

1. Create an HMR rule set (using the Global Configuration mode command *hmr rule-set <name> on page 1315*).
2. Create HMR rule(s) for the rule set (using the command *rule-set on page 4802*).
3. Specify each HMR rule's action (add, match, modify, remove using the appropriate commands in this section).
4. Optionally, configure variables for the HMR rule (using the commands *set private-variable on page 4806* and *set public-variable on page 4809*).
5. Create an HMR policy (using the Global Configuration mode command *hmr policy <name> on page 1314*).
6. Assign the HMR rule set to the appropriate HMR policy (using the command *rule-set on page 4802*).
7. Apply the HMR policy to the appropriate SIP traffic (using the Global Configuration mode commands *sip hmr on page 1723* and *sip proxy hmr on page 1750*).

The commands covered in this section include those executed from the SIP HMR Policy Configuration mode, the HMR Rule Set Configuration mode, and the HMR Message Rule Configuration mode. For more information about using SIP HMR, refer to the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76

To create a SIP HMR policy, and enter the SIP HMR Policy Configuration mode, enter the **hmr policy** <*name*> parameter from the Global Configuration mode as follows:

```
(config)#hmr policy POLICY1
(config-policy-POLICY1)#
```

The commands available in the HMR Policy Configuration mode are listed in alphabetical order below:

rule-set on page 4802

To create a SIP HMR rule set, and enter the HMR Rule Set Configuration mode, enter the **hmr rule-set** <*name*> command from the Global Configuration mode as follows:

```
(config)#hmr rule-set SET1
(config-rule-set-SET1)#
```

The commands available in the HMR Rule Set Configuration mode are listed in alphabetical order below:

message-rule on page 4791

To configure the actions of the HMR message rules, enter the HMR Message Rule Configuration mode by entering the **message-rule** command from the HMR Rule Set Configuration mode as follows:

```
(config)#hmr rule-set SET1
(config-rule-set-SET1)#message-rule RULE1 message-type any 5
(config-msg-rule-RULE1)#
```

The commands available in the HMR Message Rule Configuration mode are listed in alphabetical order below:

add header position

Use the **add header position** command from the Message Rule Set Configuration mode to add headers to Session Initiation Protocol (SIP) messages using SIP header manipulation. Use the **no** form of this command to remove the header addition rule from the rule set. Variations of this command include:

add header <*header*> **position first new-value** <*value string*>
add header <*header*> **position first new-value** <*value string*> <*sequence number*>
add header <*header*> **position if-not-present new-value** <*value string*>
add header <*header*> **position if-not-present new-value** <*value string*> <*sequence number*>
add header <*header*> **position last new-value** <*value string*>
add header <*header*> **position last new-value** <*value string*> <*sequence number*>

Syntax Description

<*header*>	Specifies the SIP header type that you want to add to the SIP message. Header types are outlined in the *Functional Notes* below.
first	Specifies that the new header is added as the first header of the specified header type within the SIP message.
if-not-present	Specifies that the new header is added only if the specified header type is not already present within the SIP message.
last	Specifies that the new header is added as the last of the specified header type within the SIP message.
new-value <*value string*>	Specifies the value to assign to the new header and is expressed as a text string. Text strings must be enclosed in quotation marks.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no SIP headers are configured for addition to SIP messages. When configured, if no sequence number is given, the rules are sequenced in increments of 10, and all rules are processed in sequence.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Multiple headers of the same type can occur in SIP messages, and therefore, the specified position of the header can determine whether a match occurs. For more information, refer to *Appendix B: Matching Regular Expressions in SIP Messages with Multiples of the Same Header* in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

SIP headers available for matching include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding
Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported
To	Via	<*name*> (specifies another header not listed here)

SIP headers can also be expressed in compact form in a SIP message. Compact forms of the header name will match the full SIP header name.

Usage Examples

The following example adds a new SIP header **Proprietary1** to the SIP message from the HMR Message Rule Configuration mode:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#add header Propietary1 position first new-value “localID=unit195;remoteID=unit272”**

all

Use the **all** command from the Message Rule Set Configuration mode to specify that a Session Initiation Protocol (SIP) header manipulation rule (HMR) is executed only if all tests in the condition block evaluate as true. Use the **no** version of this command to remove the action. Variations of this command include:

all
all <*sequence number*>

Syntax Description

<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

If the **all** command is present in the message rule's configuration, the message rule is processed only if all the stated conditions in the condition block are resolved as true. The condition blocks also use the command *end on page 4775* which signifies the end of the conditions that must be met.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to be applied if all configured conditions are resolved to true. In this case, the rule is configured to match based on the SIP Via and Identity headers and to modify the body of messages with both those headers. These actions are carried out if all the conditions are met.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#all**
(config-msg-rule-RULE1)**#match header via**
(config-msg-rule-RULE1)**#match header identity**
(config-msg-rule-RULE1)**#end-all**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

any

Use the **any** command from the Message Rule Set Configuration mode to specify that a Session Initiation Protocol (SIP) header manipulation rule (HMR) is executed if any of the configured conditions in the condition block are met. Use the **no** version of this command to remove the action. Variations of this command include:

any
any <*sequence number*>

Syntax Description

<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

If the **any** command is present in the message rule's configuration, the message rule is processed if any of the previously stated conditions in the condition block are resolved as true.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to be applied if any configured conditions are resolved to true. In this case, the rule is configured to match both the SIP Via and Identity headers, and then to modify the body of messages with either header. These actions are carried out if either of the conditions are met.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#any**
(config-msg-rule-RULE1)**#match header via**
(config-msg-rule-RULE1)**#match header identity**
(config-msg-rule-RULE1)**#end-any**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

compare

Use the **compare** command from the Message Rule Set Configuration mode to compare two string values when using Session Initiation Protocol (SIP) header manipulation rule (HMR). These comparisons are used within condition blocks to determine whether HMR rules are applied. Use the **no** version of this command to remove the action. Variations of this command include:

compare <*"string"*> **equal** <*"string"*>
compare <*"string"*> **equal** <*"string"*> <*sequence number*>
compare <*"string"*> **greater-equal** <*"string"*>
compare <*"string"*> **greater-equal** <*"string"*> <*sequence number*>
compare <*"string"*> **greater** <*"string"*>
compare <*"string"*> **greater** <*"string"*> <*sequence number*>
compare <*"string"*> **less-equal** <*"string"*>
compare <*"string"*> **less-equal** <*"string"*> <*sequence number*>
compare <*"string"*> **less** <*"string"*>
compare <*"string"*> **less** <*"string"*> <*sequence number*>
compare <*"string"*> **not-equal** <*"string"*>
compare <*"string"*> **not-equal** <*"string"*> <*sequence number*>

Syntax Description

<*"string"*>	Specifies the text string to be used for comparison. Text strings should be enclosed in quotation marks.
equal	Specifies the condition is returned true if the first expression is equal to the second expression.
greater-equal	Specifies the condition is returned true if the first expression is greater than or equal to the second expression.
greater	Specifies the condition is returned true if the first expression is greater than the second expression.
less-equal	Specifies the condition is returned true if the first expression is less than or equal to the second expression.
less	Specifies the condition is returned true if the first expression is less than the second expression.
not-equal	Specifies the condition is returned true if the first expression is not equal to the second expression.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The **compare** command is used to compare two string expressions. The comparison results in a true or false logical condition, which in turn causes other HMR rules to be enforced or discarded based on the rule's configured condition blocks.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to be applied if the string comparison conditions are resolved to true. In this case, the rule is configured to compare two strings for equality, and then modify the SIP header if the text strings are equal.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#compare "teststring1" equal "teststring2"**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

else

Use the **else** command from the Message Rule Set Configuration mode to specify an alternative action is taken by a Session Initiation Protocol (SIP) header manipulation rule (HMR) when the condition block returns false. Use the **no** version of this command to remove the action. Variations of this command include:

else
else <*sequence number*>

Syntax Description

<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The **else** command is used to specify alternative processing for conditional failure within the HMR rule's configuration, and is used in conjunction with the command *if on page 4781*. The **if** command specifies an action to be taken if specified conditions resolve as true, and the optional **else** command specifies alternative actions if the specified conditions resolve as false. The conditional block ends with the **end-if** command.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to perform a body modification on a SIP message who's header matches the Sip-Req-Uri header if the condition block (in the following example, a comparison) returns false.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#match header sip-req-uri match-value /^REFER.*/**
(config-rule-set-SET1)**#if**
(config-msg-rule-RULE1)**#compare "teststring1" equal "teststring2"**
(config-msg-rule-RULE1)**#else**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

end

Use the **end** command from the Message Rule Set Configuration mode to signal the end of a condition block in Session Initiation Protocol (SIP) header manipulation rule (HMR) configuration. Use the **no** version of this command to remove the action. Variations of this command include:

end-all
end-all <*sequence number*>
end-any
end-any <*sequence number*>
end-for
end-for <*sequence number*>
end-if
end-if <*sequence number*>
end-not
end-not <*sequence number*>

Syntax Description

all	Specifies the end of an **all** condition block. Refer to the command *all on page 4767*.
any	Specifies the end of an **any** condition block. Refer to the command *any on page 4769*.
for	Specifies the end of a **for** condition block. Refer to the command *for on page 4779*.
if	Specifies the end of an **if** condition block. Refer to the command *if on page 4781*.
not	Specifies the end of a **not** condition block. Refer to the command *not on page 4797*.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured. When a conditional block is configured, the default condition is **all**.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The **end** commands are used in conjunction with the conditional block commands **all**, **any**, **for**, **if**, and **not**. These commands are entered to signal the beginning of a block of actions taken based on the conditional logic specified by the command, and the **end** version is used to signal the end of the block of conditional logic. Only the criteria specified between the two commands is used for the conditional logic of that block. These commands take the results of a true or false logical condition, and enforce or discard other HMR rules based on the rule's configuration. If the conditional block commands (**all**, **any**, or **not**) are not specified, **all** is used by default and the **end** command does not need to be entered.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to perform a match on a SIP header, and if the match condition is true, to then modify the body of the message.The **end-if** command is used to specify the end of the actions taken based on the logical **if**.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#match header sip-req-uri match-value /^REFER.*/**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

evaluate

Use the **evaluate** command from the Message Rule Set Configuration mode to trigger an expression evaluation within the Session Initiation Protocol (SIP) header manipulation rule (HMR) condition block configuration. Use the **no** version of this command to remove the action. Variations of this command include:

evaluate *<pattern>*
evaluate *<pattern> <sequence number>*

Syntax Description

<pattern>	Specifies the expression to evaluate. This can be a regular expression or a text string, and can reference variable names. A text string must be enclosed in quotation marks.
<sequence number>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The **evaluate** command is used to trigger the evaluation of a specific expression. If the expression can be executed, the results of the evaluation are true. If the expression cannot be executed, the results of the evaluation are false. This command allows HMR rules to be enforced or discarded within the condition block based on the results of the evaluation.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to evaluate the text string **teststring1**, and perform a body modification on the SIP message if the evaluation results are returned true.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#evaluate teststring1**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

for

Use the **for** command from the Message Rule Set Configuration mode to configure a loop of conditional logic or specific actions for the specified Session Initiation Protocol (SIP) header or variable in the header manipulation rule (HMR) configuration. Use the **no** version of this command to remove the loop. Variations of this command include:

for callid-variable <*name*>
for callid-variable <*name*> <*sequence number*>
for header <*header*>
for header <*header*> <*sequence number*>
for private-variable <*name*>
for private-variable <*name*> <*sequence number*>
for public-variable <*name*>
for public-variable <*name*> <*sequence number*>

Syntax Description

callid-variable	Specifies that a processing loop will be created for a call ID variable.
header <*header*>	Specifies the SIP header type for which you want to create the processing loop. Header types are outlined in the *Functional Notes* below.
private-variable	Specifies that a processing loop is created for a private variable.
public-variable	Specifies that a processing loop is created for a public variable.
<*name*>	Specifies the name of the variable for which you want to create the processing loop.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of 10, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.
Release R12.2.0	Command was expanded to include the **callid-variable**, **private-variable**, and **public-variable** parameters.

Functional Notes

SIP headers available for loop processing include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding

Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-Info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported
To	Via	<*name*> (specifies another header not listed here)

When a header or variable is specified using the **for** command, a **for** processing loop is created for the specified header or variable. This loop can specify actions, such as header modification or variable configurations, or conditional blocks to be applied to the specified header. The command is used in conjunction with the **end-for** command (refer to *end on page 4775*), which signals the end of the processing block.

Usage Examples

The following example configures the HMR rule **RULE1** to create a processing loop for the Via header. The processing loop sets the private variable **VAR1** for the header. The **end-for** command specifies the end of the processing loop for that header.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#for header Via**
(config-msg-rule-RULE1)**#set private variable VAR1**
(config-msg-rule-RULE1)**#end-for**

if

Use the **if** command from the Message Rule Set Configuration mode to specify an action is taken by a Session Initiation Protocol (SIP) header manipulation rule (HMR) when the condition block returns as true. Use the **no** version of this command to remove the action. Variations of this command include:

if
if <*sequence number*>

Syntax Description

<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The **if** command is used to specify the beginning of a condition block within the HMR rule's configuration, and is used in conjunction with the commands **if** and **else**. The **if** command specifies an action to be taken if specified conditions resolve as true, and the optional **else** command specifies alternative actions if the specified conditions resolve as false. The conditional block ends with the **end-if** command.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to perform a body modification on a SIP message who's header matches the SIP Identity header, if the condition block (in the following example, a comparison) returns true.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#match header identity**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#compare "teststring1" equal "teststring2"**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

int-compare

Use the **int-compare** command from the Message Rule Set Configuration mode to compare two integer values when using Session Initiation Protocol (SIP) header manipulation rule (HMR). These comparisons are used to determine whether other configured HMR rules are applied by condition blocks. Use the **no** version of this command to remove the action. Variations of this command include:

int-compare <*pattern*> **equal** <*pattern*>
int-compare <*pattern*> **equal** <*pattern*> <*sequence number*>
int-compare <*pattern*> **greater-equal** <*pattern*>
int-compare <*pattern*> **greater-equal** <*pattern*> <*sequence number*>
int-compare <*pattern*> **greater** <*pattern*>
int-compare <*pattern*> **greater** <*pattern*> <*sequence number*>
int-compare <*pattern*> **less-equal** <*pattern*>
int-compare <*pattern*> **less-equal** <*pattern*> <*sequence number*>
int-compare <*pattern*> **less** <*pattern*>
int-compare <*pattern*> **less** <*pattern*> <*sequence number*>
int-compare <*pattern*> **not-equal** <*pattern*>
int-compare <*pattern*> **not-equal** <*pattern*> <*sequence number*>

Syntax Description

<*pattern*>	Specifies the expression to be used for comparison. This can be a test string, a regular expression, a variable, or a variable function. Text strings should be enclosed in quotation marks. This pattern returns an integer value for HMR processing.
equal	Specifies the condition is returned true if the first expression is equal to the second expression.
greater-equal	Specifies the condition is returned true if the first expression is greater than or equal to the second expression.
greater	Specifies the condition is returned true if the first expression is greater than the second expression.
less-equal	Specifies the condition is returned true if the first expression is less than or equal to the second expression.
less	Specifies the condition is returned true if the first expression is less than the second expression.
not-equal	Specifies the condition is returned true if the first expression is not equal to the second expression.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

The **int-compare** command is used to compare two integer expressions. The integer value is derived from the information contained in the expression. The comparison results in a true or false logical condition, which in turn causes other HMR rules to be enforced or discarded based on the rule's configured condition blocks.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to be applied if the expression comparison conditions are resolved to true. In this case, the rule is configured to compare two expressions for equality, judged on the integer value, and then to modify the SIP header if the expressions are equal.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#int-compare "teststring1" equal "teststring2"**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**

match body

Use the **match body** command from the Message Rule Set Configuration mode to specify a Session Initiation Protocol (SIP) message body to match in SIP messages using SIP header manipulation rules (HMR). Match commands allow you to specify conditions that must be true in order for the SIP message rule to be processed. Use the **no** form of this command to remove the message body matching rule from the rule set. Variations of this command include:

match body
match body match-value <*pattern*>

Syntax Description

match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names.

Default Values

By default, no message body matching rules are configured.

Command History

Release R11.3.0	Command was introduced.

Usage Examples

The following example specifies that the HMR rule matches the body of a SIP message when it contains the pattern **PATTERN1**:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#match body match-value /PATTERN1/**

match call-variable

Use the **match call-variable** command to match a Session Initiation Protocol (SIP) message based on a previously configured call ID variable when using SIP header manipulation rules (HMR). Call ID variables are created based on the call ID from SIP messages. Use the **no** form of this command to remove the variable matching rule from the HMR message rule set. Variations of this command include:

match call-variable <*variable*>
match call-variable <*variable*> **match-value** <*pattern*>

Syntax Description

<*variable*>	Specifies a previously created call ID variable to use for matching. Call ID variables are expressed in the format **%callid.myVariable%**.
match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names. A text string must be enclosed in quotation marks.

Default Values

By default, no call ID variables are configured.

Command History

Release R12.1.0	Command was introduced.

Functional Notes

If a pattern value is specified, the variable must contain the specified value in order for the rule to be processed. If the pattern is not specified, the match resolves as true if the variable is defined.

Call ID variable storage for a given call ID is limited to the lifetime of the associated call structure or lifetime of the SIP proxy call. Call ID variable storage for a non-call call ID is limited to 20 seconds beyond the last detected usage of the variable associated with the call ID.

Usage Examples

The following example creates a rule to match the call ID variable **callid.myUnitNumber** with a pattern of **253**:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#match call-variable calllid.myUnitNumber match-value “253”**

match header

Use the **match header** command from the Message Rule Set Configuration mode to specify a Session Initiation Protocol (SIP) header to match in SIP messages using SIP header manipulation rules (HMR). Match commands allow you to specify conditions that must be true in order for the SIP message rule to be processed. Use the **no** form of this command to remove the header matching rule from the rule set. Variations of this command include:

match header <*header*>
match header <*header*> **match-value** <*pattern*>

Syntax Description

<*header*>	Specifies the SIP header type in the SIP message that you want to match. Header types are outlined in the *Functional Notes* below.
match-value <*pattern*>	Optional. Specifies the pattern to be used for header matching. This can be a regular expression or a text string, and can reference variable names. A text string must be enclosed in quotation marks.

Default Values

By default, no header matching rules are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

If a **match header** command is present in the message rule's configuration, the message rule is processed only if the **match header** resolves as true. Multiple match header commands can be present in a message rule, but all of them must resolve as true for the message rule to be processed.

SIP headers available for matching include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding
Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported

To	Via	<*name*> (specifies another header not listed here)

SIP headers can also be expressed in compact form in a SIP message. Compact forms of the header name will match the full SIP header name.

If both the header and a match pattern are specified, the indicated SIP header must be present in the SIP message and must contain the specified pattern for the rule to resolve as true. If only the SIP header is specified, the SIP message must contain the specified SIP header for the rule to resolve as true.

Usage Examples

The following example specifies that the HMR rule matches SIP headers based on a specific header and the pattern in REFER requests:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#match header sip-req-uri match-value /^REFER.*/**

match private-variable

Use the **match private-variable** command to match a Session Initiation Protocol message based on a previously configured private variable when using SIP header manipulation rules (HMR). Private variables are configured using the command *set private-variable on page 4806*. Use the **no** form of this command to remove the variable matching rule from the HMR message rule set. Variations of this command include:

match private-variable <*variable*>
match private-variable <*variable*> **match-value** <*pattern*>

Syntax Description

<*variable*>	Specifies a previously configured variable to use for matching. Variables are expressed in the format **%private.VariableName%**.
match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names. A text string must be enclosed in quotation marks.

Default Values

By default, no private variables are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

If a pattern value is specified, the variable must contain the specified value in order for the rule to be processed. If the pattern is not specified, the match resolves as true if the variable is defined.

Usage Examples

The following example creates a rule to match the private variable **myUnitNumber** with a pattern of **253**:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#match private-variable myUnitNumber match-value “253”**

match public-variable

Use the **match public-variable** command to match a Session Initiation Protocol message based on a previously configured public variable when using SIP header manipulation rules (HMR). Public variables are configured using the command *set public-variable on page 4809*. Use the **no** form of this command to remove the variable matching rule from the HMR message rule set. Variations of this command include:

match public-variable <*variable*>
match public-variable <*variable*> **match-value** <*pattern*>

Syntax Description

<*variable*>	Specifies a previously configured variable to use for matching. Variables are expressed in the format **%public.VariableName%**.
match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names. Text strings must be enclosed in quotation marks.

Default Values

By default, no public variables are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

If a pattern value is specified, the variable must contain the specified value in order for the rule to be processed. If the pattern is not specified, the match resolves as true if the variable is defined.

Usage Examples

The following example creates a rule to match the public variable **myUnitNumber** with a pattern of **262**:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#match private-variable myUnitNumber match-value “262”**

message-rule

Use the **message-rule** command from the Session Initiation Protocol (SIP) header manipulation rule (HMR) Rule Set Configuration mode to create a message rule for the rule set, and enter the message rule's configuration mode. This command specifies the type of messages to which the manipulation rules are applied. Use the **no** form of this command to remove the message rule. Variations of this command include:

message-rule <*name*>
message-rule <*name*> <*sequence number*>
message-rule <*name*> **message-type any**
message-rule <*name*> **message-type any** <*sequence number*>
message-rule <*name*> **message-type request**
message-rule <*name*> **message-type request** <*sequence number*>
message-rule <*name*> **message-type response**
message-rule <*name*> **message-type response** <*sequence number*>

Syntax Description

<*name*>	Specifies the name of the message rule. Message rule names must be unique within the HMR rule set.
message-type any	Optional. Specifies that the message rule is applied to both SIP request and response messages.
message-type request	Optional. Specifies that the message rule is applied to SIP request messages.
message-type response	Optional. Specifies that the message rule is applied to SIP response messages.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no message rules are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

A message rule is a collection of one or more header commands, which determine the types of SIP headers to act upon, and the action to be taken. When a message rule is applied to a SIP message, all matching header commands are processed. Message rules are processed in the order determined by the sequence number of the message rule within the rule set. When multiple rules are applied to a message, the results of each rule are applied before the next rule is evaluated and applied.

Usage Examples

The following example creates a message rule named **RULE1** that applies to **any** SIP message type and has a sequence number of **5**. In addition, the example enters the rule's configuration mode:

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)#

modify body

Use the **modify body** command to use Session Initiation Protocol (SIP) header manipulation rules (HMR) to modify the body of a SIP message. This command is entered from the HMR Message Rule Set Configuration mode. Use the **no** form of this command to remove the rule from the message rule set. Variations of this command include:

modify body match-value <*pattern*> **new-value** <*pattern*>
modify body match-value <*pattern*> **new-value** <*pattern*> <*sequence number*>
modify body new-value <*pattern*>
modify body new-value <*pattern*> <*sequence number*>

Syntax Description

match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names.
new-value <*pattern*>	Specifies the value to be assigned to the SIP message body. This can be a regular expression or a text string. Text strings must be enclosed in quotation marks.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no message body manipulation rules are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

If the match pattern is provided, the content of the message is only modified if the message contains the specified match pattern. If no match pattern is specified, the message body is modified unconditionally.

When the SIP message body is modified, SIP HMR automatically adjusts the Content-Length header of the message to match the length of the new value.

Usage Examples

The following example specifies that body of a SIP message is modified when it matches the variable **PATTERN1**:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**

modify header position

Use the **modify header position** command from the Session Initiation Protocol (SIP) header manipulation rule (HMR) Message Rule Set Configuration mode to specify a SIP header to modify. Use the **no** form of this command to remove the header modification rule from the rule set. Variations of this command include:

modify header <*header*> **position all new-value** <*pattern*>
modify header <*header*> **position all new-value** <*pattern*> <*sequence number*>
modify header <*header*> **position all match-value** <*pattern*> **new-value** <*pattern*>
modify header <*header*> **position all match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
modify header <*header*> **position first new-value** <*pattern*>
modify header <*header*> **position first new-value** <*pattern*> <*sequence number*>
modify header <*header*> **position first match-value** <*pattern*> **new-value** <*pattern*>
modify header <*header*> **position first match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
modify header <*header*> **position first-match new-value** <*pattern*>
modify header <*header*> **position first-match new-value** <*pattern*> <*sequence number*>
modify header <*header*> **position first-match match-value** <*pattern*> **new-value** <*pattern*>
modify header <*header*> **position first-match match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
modify header <*header*> **position last new-value** <*pattern*>
modify header <*header*> **position last new-value** <*pattern*> <*sequence number*>
modify header <*header*> **position last match-value** <*pattern*> **new-value** <*pattern*>
modify header <*header*> **position last match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>

Syntax Description

<*header*>	Specifies the SIP header type in the SIP message that you want to modify. Header types are outlined in the *Functional Notes* below.
all	Specifies that all matching headers of the specified type are modified.
first	Specifies that the first header of the specified type is modified.
first-match	Specifies that the first matching header of the specified header type, regardless of its position within the message, is modified.
last	Specifies the last header of the specified type is modified.
match-value <*pattern*>	Optional. Specifies the pattern to be used for header matching. This can be a regular expression or a text string, and can reference variable names.
new-value <*pattern*>	Specifies the value to be assigned to the header. This can be a regular expression or a text string.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no SIP headers are modified.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Multiple headers of the same type can occur in SIP messages, and therefore, the specified position of the header can determine whether a match occurs. For more information, refer to *Appendix B: Matching Regular Expressions in SIP Messages with Multiples of the Same Header* in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

SIP headers available for matching include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding
Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported
To	Via	<*name*> (specifies another header not listed here)

SIP headers can also be expressed in compact form in a SIP message. Compact forms of the header name will match the full SIP header name.

If both the header and a match pattern are specified, the indicated SIP header must be present in the SIP message and must contain the specified pattern for the rule to resolve as true. If only the SIP header is specified, the SIP message must contain the specified SIP header for the rule to resolve as true.

Usage Examples

The following example modifies the Contact header in the SIP message by adding **<>** to Contact headers that do not contain them:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#modify header contact position all match-value /([^<]*)(sip:.*@.*[^;])(.*/ new-value /\1<\2>\3/**

not

Use the **not** command from the Message Rule Set Configuration mode to specify that a Session Initiation Protocol (SIP) header manipulation rule (HMR) is executed after a test for the negative of the configured logical block conditions. Use the **no** version of this command to remove the action. Variations of this command include:

not
not <*sequence number*>

Syntax Description

<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no header manipulation rules are configured.

Command History

Release R11.10.0	Command was introduced.

Functional Notes

If the **not** command is present in the message rule's configuration, the message rule is processed if any of the previously stated conditions in the condition block are resolved as false. The condition blocks also use the command *end on page 4775*, which signifies the end of the conditions that must be met.

The condition block is entered using the **if** or **for** commands (refer to the commands *if on page 4781* and *for on page 4779*), which signify the beginning of the logical block. The logical block is configured to discard or enforce HMR actions (such as modifying, adding, or removing headers, etc.) based on the use of the **not**, **all**, or **any** logical commands. Additionally, the **compare** and **evaluate** commands can be used in an **if** block to specify whether conditional logic criteria are met by comparing or evaluating specified criteria. Based on the logical commands contained within the block, HMR actions are enforced or discarded according to the configured action.

Usage Examples

The following example configures the HMR rule **RULE1** to be applied if any configured conditions are resolved to be false. In this case, the rule is configured to match both the Via header and the Identity header, and then to modify the body of messages without either header using the **not** command. Like other conditional block commands in HMR, this configuration requires the **end-not** command to signal the end of the conditional block.

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#not**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-not**
(config-msg-rule-RULE1)**#match header via**
(config-msg-rule-RULE1)**#match header identity**
(config-msg-rule-RULE1)**#end-if**

remove header position

Use the **remove header position** command to remove Session Initiation Protocol (SIP) headers from SIP messages when the header is matched using SIP header manipulation rules (HMR). This command is executed from the HMR Message Rule Set Configuration mode. Use the **no** form of this command to remove the rule from the message rule set. Variations of this command include:

remove header <*header*> **position all**
remove header <*header*> **position all** <*sequence number*>
remove header <*header*> **position all match-pattern** <*pattern*>
remove header <*header*> **position all match-pattern** <*pattern*> <*sequence number*>
remove header <*header*> **position first**
remove header <*header*> **position first** <*sequence number*>
remove header <*header*> **position first match-pattern** <*pattern*>
remove header <*header*> **position first match-pattern** <*pattern*> <*sequence number*>
remove header <*header*> **position first-match**
remove header <*header*> **position first-match** <*sequence number*>
remove header <*header*> **position first-match match-pattern** <*pattern*>
remove header <*header*> **position first-match match-pattern** <*pattern*> <*sequence number*>
remove header <*header*> **position last**
remove header <*header*> **position last** <*sequence number*>
remove header <*header*> **position last match-pattern** <*pattern*>
remove header <*header*> **position last match-pattern** <*pattern*> <*sequence number*>

Syntax Description

<*header*>	Specifies the SIP header type that you want to remove from the SIP message. Header types are outlined in the *Functional Notes* below.
all	Specifies that all matching headers of the specified type are removed.
first	Specifies that the first header of the specified type is removed.
first-match	Specifies that the first matching header of the specified header type, regardless of its position within the message, is removed.
last	Specifies the last header of the specified type is removed.
match-value <*pattern*>	Optional. Specifies the pattern to be used for header matching. This can be a regular expression or a text string, and can reference variable names.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no remove header rules are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

Multiple headers of the same type can occur in SIP messages, and therefore, the specified position of the header can determine whether a match occurs. For more information, refer to *Appendix B: Matching Regular Expressions in SIP Messages with Multiples of the Same Header* in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

SIP headers available for matching include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding
Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported
To	Via	<*name*> (specifies another header not listed here)

SIP headers can also be expressed in compact form in a SIP message. Compact forms of the header name will match the full SIP header name.

If both the header and a match pattern are specified, the indicated SIP header must be present in the SIP message and must contain the specified pattern for the rule to resolve as true. If only the SIP header is specified, the SIP message must contain the specified SIP header for the rule to resolve as true.

Usage Examples

The following example specifies that the **Proprietary1** header is removed from the first position in all SIP messages:

(config-rule-set-SET1)**#message-rule RULE1 message-type any 5**
(config-msg-rule-RULE1)**#remove header Proprietary1 position first**

renumber

Use the **renumber** command with the Session Initiation Protocol (SIP) header manipulation rules (HMR) configuration to renumber individual actions within a message rule. This command is executed from the HMR Message Rule Set Configuration mode. The new number assignments start at 10 and are incremented by 10 for each action.

Syntax Description

No subcommands.

Default Values

By default, rule actions are numbered by the order in which they were entered, in increments of 10, starting with zero (unless otherwise defined).

Command History

Release R12.2.0	Command was introduced.

Usage Examples

The following example renumbers the **if** action rules within **RULE1**:

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#match header sip-req-uri match-value /^REFER.*/**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#compare “teststring1” equal “teststring2”**
(config-msg-rule-RULE1)**#else**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**
(config-msg-rule-RULE1)**#if**
(config-msg-rule-RULE1)**#match header sip-req-uri match-value /^REFER.*/**
(config-msg-rule-RULE1)**#modify body new-value PATTERN1**
(config-msg-rule-RULE1)**#end-if**
(config-msg-rule-RULE1)**#renumber**

rule-set

Use the **rule-set** command to apply a rule set to a Session Initiation Protocol (SIP) header manipulation rule (HMR) policy. This command is executed from the HMR Policy Configuration mode. Use the **no** form of this command to remove the rule set from the policy. Variations of this command include:

rule-set <*name*>
rule-set <*name*> <*sequence number*>

Syntax Description

<*name*>	Specifies the previously created rule set that you want to apply to the HMR policy. Multiple rule sets can be added to a single policy. When multiple rule sets are applied to a policy, the results of each rule set are applied before the next rule set is evaluated and applied.
<*sequence number*>	Optional. Specifies the sequence number given to the rule set, which determines the order in which the rule sets are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no HMR rule sets are configured or applied to HMR policies.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example adds the previously created rule set **SET1** to the HMR policy **POLICY1**:

(config)**#hmr policy POLICY1**
(config-policy-POLICY1)**#rule-set SET1**

set callid-variable

Use the **set callid-variable** command to set the value of a call ID variable to use with Session Initiation Protocol (SIP) header manipulation rules (HMR) configuration. This command is executed from the HMR Message Rule Set Configuration mode. Use the **no** form of this command to delete the variable. Variations of this command include:

set callid-variable <*name*> **body match-value** <*pattern*> **new-value** <*pattern*>
set callid-variable <*name*> **body match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
set callid-variable <*name*> **header** <*header*> **position first match-value** <*pattern*> **new-value** <*pattern*>
set callid-variable <*name*> **header** <*header*> **position first match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
set callid-variable <*name*> **header** <*header*> **position first-match match-value** <*pattern*> **new-value** <*pattern*>
set callid-variable <*name*> **header** <*header*> **position first-match match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
set callid-variable <*name*> **header** <*header*> **position last match-value** <*pattern*> **new-value** <*pattern*>
set callid-variable <*name*> **header** <*header*> **position last match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
set callid-variable <*name*> **match-value** <*pattern*> **new-value** <*pattern*>
set callid-variable <*name*> **match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
set callid-variable <*name*> **new-value** <*pattern*>
set callid-variable <*name*> **new-value** <*pattern*> <*sequence number*>
set callid-variable <*name*> **new-value** <*pattern*> **match-value** <*pattern*>
set callid-variable <*name*> **new-value** <*pattern*> **match-value** <*pattern*> <*sequence number*>

Syntax Description

<*name*>	Specifies the name of the call ID variable. Call ID variables are referenced in the format **%callid.variablename%**.
body	Optional. Specifies that matching occurs on the body of the SIP message.
header <*header*>	Optional. Specifies whether the optional match pattern applies to the contents of a SIP header or to the existing contents of the variable. Available header types are outlined in the *Functional Notes* below.
match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names.
new-value <*pattern*>	Specifies the value to be assigned to the variable. This can be a regular expression or a text string.
position first	Optional. Specifies that the first header of the specified type is used as a data source for the variable.
position first-match	Optional. Specifies that the first matching header of the specified header type, regardless of its position within the message, is used as a data source for the variable.
position last	Optional. Specifies the last header of the specified type is used as a data source for the variable.

<sequence number>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of 10 and all rules are processed in sequence.

Default Values

By default, no variables are configured.

Command History

Release R12.2.0	Command was introduced.

Functional Notes

Call ID variables allow the storage and retrieval of data to and from named variables. The variables are scoped by the call ID from the SIP messages (thus preventing confusion of data between call threads). In addition, call ID information from the two separate SIP call legs within one call structure are associated with each other, allowing HMR rules to access information from both.

Call ID variables are stored for the lifetime of the associated call structure, or the lifetime of the SIP proxy call. The lifetime of a call ID variable for a given non-call call ID is limited to 20 seconds beyond the last detected usage of a variable associated with the call ID.

Multiple headers of the same type can occur in SIP messages, and therefore, the specified position of the header can determine whether a match occurs. For more information, refer to *Appendix B: Matching Regular Expressions in SIP Messages with Multiples of the Same Header* in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

SIP headers available for matching include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding
Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-Info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported
To	Via	*<name>* (specifies another header not listed here)

SIP headers can also be expressed in compact form in a SIP message. Compact forms of the header name will match the full SIP header name.

If both the header and a match pattern are specified, the indicated variable is modified if the header is present and contains the match value. If only the match pattern is specified, the match pattern is applied to the variable's current value.

In AOS firmware release R11.6.0, additional manipulation capability is included for both public and private variables. These features allow you to perform additional operations on the content of both public and private variables. These operations include (but are not limited to) appending to, deleting from, or replacing variable content as well as searching or comparing variable content. To perform these operations on variable content, manipulative actions are specified in the variable's pattern definition. When the variable is defined with one of these commands, a new value (**new-value** *<pattern>*) or a match value (**match-value** *<pattern>*) can also be defined. These values, specified in the *<pattern>* parameter, are expressed as a regular expressions or text strings. To perform additional operations on the content of the variable, you can specify an action in the *<pattern>* parameter of the new or matched value. In this case, the *<pattern>* parameter is not just a regular expression or text string, but rather a combination of the variable name and the operation you want to perform on the variable's content; it is expressed as *<variable name>.<function>*, so that, for example, **set callid-variable %CALLIDVAR1% match-value MATCH** becomes **set callid-variable %CALLIDVAR1% match-value %CALLIDVAR1%.add(1)**. The *<variable name>* parameter in this instance is the variable that contains the content to be manipulated, and the *<function>* parameter is the manipulative action to be applied to that content. Function pattern definitions are outlined in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

Usage Examples

The following example sets a call ID variable called **callID1**:

(config)**#hmr rule-set SET1**
(config-rule-set-SET1)**#message-rule RULE1**
(config-msg-rule-RULE1)**#set callid-variable callID1 new-value callID2**

set private-variable

Use the **set private-variable** command to set the value of a private variable to use with Session Initiation Protocol (SIP) header manipulation rules (HMR) configuration. Private variables are only visible within a single HMR policy. This command is executed from the HMR Message Rule Set Configuration mode. Use the **no** form of this command to delete the variable. Variations of this command include:

set private-variable <*name*> **body match-value** <*pattern*> **new-value** <*pattern*>
set private-variable <*name*> **body match-value** <*pattern*> **new-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **header** <*header*> **position first new-value** <*pattern*>
set private-variable <*name*> **header** <*header*> **position first new-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **header** <*header*> **position first new-value** <*pattern*> **match-value** <*pattern*>
set private-variable <*name*> **header** <*header*> **position first new-value** <*pattern*> **match-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **header** <*header*> **position first-match new-value** <*pattern*>
set private-variable <*name*> **header** <*header*> **position first-match new-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **header** <*header*> **position first-match new-value** <*pattern*> **match-value** <*pattern*>
set private-variable <*name*> **header** <*header*> **position first-match new-value** <*pattern*> **match-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **header** <*header*> **position last new-value** <*pattern*>
set private-variable <*name*> **header** <*header*> **position last new-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **header** <*header*> **position last new-value** <*pattern*> **match-value** <*pattern*>
set private-variable <*name*> **header** <*header*> **position last new-value** <*pattern*> **match-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **new-value** <*pattern*>
set private-variable <*name*> **new-value** <*pattern*> <*sequence number*>
set private-variable <*name*> **new-value** <*pattern*> **match-value** <*pattern*>
set private-variable <*name*> **new-value** <*pattern*> **match-value** <*pattern*> <*sequence number*>

Syntax Description

<*name*>	Specifies the name of the variable. Variables are referenced in the format **%private.variablename%**.
body	Optional. Specifies that the match pattern applies to the body of the SIP message.
header <*header*>	Optional. Specifies whether the optional match pattern applies to the contents of a SIP header or to the existing contents of the variable. Available header types are outlined in the *Functional Notes* below.
position first	Optional. Specifies that the first header of the specified type is used as a data source for the variable.
position first-match	Optional. Specifies that the first matching header of the specified header type, regardless of its position within the message, is used as a data source for the variable.

position last	Optional. Specifies the last header of the specified type is used as a data source for the variable.
match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names.
new-value <*pattern*>	Specifies the value to be assigned to the variable. This can be a regular expression or a text string.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no variables are configured.

Command History

Release R10.1.0	Command was introduced.
Release R11.3.0	Command was expanded to include the **body** parameter.
Release R11.6.0	Command was expanded to include variable manipulation in the <*pattern*> parameter.

Functional Notes

Multiple headers of the same type can occur in SIP messages, and therefore, the specified position of the header can determine whether a match occurs. For more information, refer to *Appendix B: Matching Regular Expressions in SIP Messages with Multiples of the Same Header* in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

SIP headers available for matching include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding
Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported
To	Via	<*name*> (specifies another header not listed here)

SIP headers can also be expressed in compact form in a SIP message. Compact forms of the header name will match the full SIP header name.

If both the header and a match pattern are specified, the indicated variable is modified if the header is present and contains the match value. If only the match pattern is specified, the match pattern is applied to the variable's current value.

In AOS firmware release R11.6.0, additional manipulation capability is included for both public and private variables. These features allow you to perform additional operations on the content of both public and private variables. These operations include (but are not limited to) appending to, deleting from, or replacing variable content as well as searching or comparing variable content. To perform these operations on variable content, manipulative actions are specified in the variable's pattern definition. When the variable is define with one of these commands, a new value (**new-value** *<pattern>*) or a match value (**match-value** *<pattern>*) can also be defined. These values, specified in the *<pattern>* parameter, are expressed as a regular expressions or text strings. To perform additional operations on the content of the variable, you can specify an action in the *<pattern>* parameter of the new or matched value. In this case, the *<pattern>* parameter is not just a regular expression or text string, but rather a combination of the variable name and the operation you want to perform on the variable's content; it is expressed as *<variable name>.<function>*, so that, for example, **set private-variable %PRIVATEVAR1% match-value MATCH** becomes **set private-variable %PRIVATEVAR1% match-value %PRIVATEVAR1%.add(1)**. The *<variable name>* parameter in this instance is the variable that contains the content to be manipulated, and the *<function>* parameter is the manipulative action to be applied to that content. Function pattern definitions are outlined in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

Usage Examples

The following example sets a private variable called **UNITID** that holds the value of the unit ID parameter from the **target-unit** header of the SIP message:

```
(config-rule-set-SET1)#message-rule RULE1 message-type any 5
(config-msg-rule-RULE1)#set private-variable UNITID header target-unit position first match-value
    /.*unitID=(.*)/ new-value /\1/
```

The following example manipulates the **inviteCount** private variable:

```
(config)#hmr rule-set INVITECOUNT
(config-rule-set-INVITECOUNT)#message-rule TestAdd1
(config-msg-rule-TestAdd1)#match header sip-req-uri match-value /INVITE/
(config-msg-rule-TestAdd1)#set private-variable inviteCount new-value
    /%public.inviteCount%.add(1)/
(config-msg-rule-TestAdd1)#exit
(config-rule-set-INVITECOUNT)#message-rule TestAdd2
(config-msg-rule-TestAdd2)#match private-variable match-value /10/
(config-msg-rule-TestAdd2)#add header MyInviteNotification position first new-value "INVITE count
    just hit 10!"
```


set public-variable

Use the **set public-variable** command to set the value of a public variable to use with Session Initiation Protocol (SIP) header manipulation rules (HMR) configuration. This command is executed from the HMR Message Rule Set Configuration mode. However, you can also configure public variables using the command *hmr set public-variable <variable> new-value <pattern> on page 1316*. Use the **no** form of this command to delete the variable. Variations of this command include:

set public-variable *<name>* **body match-value** *<pattern>* **new-value** *<pattern>*
set public-variable *<name>* **body match-value** *<pattern>* **new-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **header** *<header>* **position first new-value** *<pattern>*
set public-variable *<name>* **header** *<header>* **position first new-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **header** *<header>* **position first new-value** *<pattern>* **match-value** *<pattern>*
set public-variable *<name>* **header** *<header>* **position first new-value** *<pattern>* **match-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **header** *<header>* **position first-match new-value** *<pattern>*
set public-variable *<name>* **header** *<header>* **position first-match new-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **header** *<header>* **position first-match new-value** *<pattern>* **match-value** *<pattern>*
set public-variable *<name>* **header** *<header>* **position first-match new-value** *<pattern>* **match-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **header** *<header>* **position last new-value** *<pattern>*
set public-variable *<name>* **header** *<header>* **position last new-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **header** *<header>* **position last new-value** *<pattern>* **match-value** *<pattern>*
set public-variable *<name>* **header** *<header>* **position last new-value** *<pattern>* **match-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **new-value** *<pattern>*
set public-variable *<name>* **new-value** *<pattern>* *<sequence number>*
set public-variable *<name>* **new-value** *<pattern>* **match-value** *<pattern>*
set public-variable *<name>* **new-value** *<pattern>* **match-value** *<pattern>* *<sequence number>*

Syntax Description

<name>	Specifies the name of the variable. Variables are referenced in the format **%public.variablename%**.
body	Optional. Specifies that matching occurs on the body of the SIP message.
header *<header>*	Optional. Specifies whether the optional match pattern applies to the contents of a SIP header or to the existing contents of the variable. Available header types are outlined in the *Functional Notes* below.
position first	Optional. Specifies that the first header of the specified type is used as a data source for the variable.
position first-match	Optional. Specifies that the first matching header of the specified header type, regardless of its position within the message, is used as a data source for the variable.

position last	Optional. Specifies the last header of the specified type is used as a data source for the variable.
match-value <*pattern*>	Optional. Specifies the pattern to be used for matching. This can be a regular expression or a text string, and can reference variable names.
new-value <*pattern*>	Specifies the value to be assigned to the variable. This can be a regular expression or a text string.
<*sequence number*>	Optional. Specifies the sequence number given to the message rule, which determines the order in which the rules are processed. Valid sequence number range is **1** to **99999**. By default, sequence numbering occurs in increments of **10**, and all rules are processed in sequence.

Default Values

By default, no variables are configured.

Command History

Release R10.1.0	Command was introduced.
Release R11.3.0	Command was expanded to include the **body** parameter.
Release R11.6.0	Command was expanded to include variable manipulation in the <*pattern*> parameter.

Functional Notes

Multiple headers of the same type can occur in SIP messages, and therefore, the specified position of the header can determine whether a match occurs. For more information, refer to *Appendix B: Matching Regular Expressions in SIP Messages with Multiples of the Same Header* in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

SIP headers available for matching include the following:

Accept-Contact	Allow	Allow-Events
Call-Id	Contact	Content-Encoding
Content-Length	Content-Type	Diversion
Event	From	Identity
Identity-info	P-Asserted-Identity	P-Preferred-Identity
Record-Route	Refer-To	Referred-By
Reject-Contact	Replaces	Request-Disposition
Route	Session-Expires	Sip-Req-Uri
Sip-Status-Line	Subject	Supported
To	Via	<*name*> (specifies another header not listed here)

SIP headers can also be expressed in compact form in a SIP message. Compact forms of the header name will match the full SIP header name.

If both the header and a match pattern are specified, the indicated variable is modified if the header is present and contains the match value. If only the match pattern is specified, the match pattern is applied to the variable's current value.

In AOS firmware release R11.6.0, additional manipulation capability is included for both public and private variables. These features allow you to perform additional operations on the content of both public and private variables. These operations include (but are not limited to) appending to, deleting from, or replacing variable content as well as searching or comparing variable content. To perform these operations on variable content, manipulative actions are specified in the variable's pattern definition. When the variable is define with one of these commands, a new value (**new-value** *<pattern>*) or a match value (**match-value** *<pattern>*) can also be defined. These values, specified in the *<pattern>* parameter, are expressed as a regular expressions or text strings. To perform additional operations on the content of the variable, you can specify an action in the *<pattern>* parameter of the new or matched value. In this case, the *<pattern>* parameter is not just a regular expression or text string, but rather a combination of the variable name and the operation you want to perform on the variable's content; it is expressed as *<variable name>.<function>*, so that, for example, **set private-variable %PRIVATEVAR1% match-value MATCH** becomes **set private-variable %PRIVATEVAR1% match-value %PRIVATEVAR1%.add(1)**. The *<variable name>* parameter in this instance is the variable that contains the content to be manipulated, and the *<function>* parameter is the manipulative action to be applied to that content. Function pattern definitions are outlined in the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at http://supportforums.adtran.com.

Usage Examples

The following example sets a public variable called **paiTest** :

```
(config-rule-set-SET1)#message-rule RULE1 message-type any 5
(config-msg-rule-RULE1)#set public-variable paiTest new-value match
```

The following example manipulates the **inviteCount** public variable:

```
(config)#hmr rule-set INVITECOUNT
(config-rule-set-INVITECOUNT)#message-rule TestAdd1
(config-msg-rule-TestAdd1)#match header sip-req-uri match-value /INVITE/
(config-msg-rule-TestAdd1)#set public-variable inviteCount new-value /%public.inviteCount%.add(1)/
(config-msg-rule-TestAdd1)#exit
(config-rule-set-INVITECOUNT)#message-rule TestAdd2
(config-msg-rule-TestAdd2)#match public-variable match-value /10/
(config-msg-rule-TestAdd2)#add header MyInviteNotification position first new-value "INVITE count
    just hit 10!"
```

HMR INTERCEPT COMMAND SET

Header manipulation rules (HMR) intercept is an AOS feature that allows standard HMR policies to be used to alter the flow of selected SIP requests. HMR intercept policies, when created and enabled, are given first access to inbound SIP requests. These policies can be used to respond to a request, block the processing of a request, or modify a request before other SIP agents within the device gain control of the request. The HMR intercept policy's rules are evaluated to determine whether one or more rules match a given SIP request. If a match occurs, all rules that match within the policy are applied to the traffic in the same way that inbound or outbound HMR policies are applied. In addition, HMR intercept actions assigned to the intercept policy are applied to the SIP request.

Three HMR intercept actions are available: modifying requests, responding to requests, and blocking requests. The respond and block actions, when invoked, take ownership of the SIP request and no other SIP agent within the AOS device is given access to the request. The modify action, when invoked, applies the assigned policy to the request but does not take ownership of the request.

Each HMR intercept action specifies an HMR intercept policy. Respond policies accept a matching request and send the specified response. The configuration of the respond policy can specify the response code as well as any text to be used in the response. The generated responses are modified by applicable rules that are included in the response policy. Block policies accept matching requests and terminate these requests without generating a response. Modify policies apply the rules included in the policy to the request. Requests are modified before other SIP agents within the AOS device gain access to the request; however, once the policy is applied, normal SIP request processing continues.

Multiple actions can be specified for an HMR intercept policy. In addition, multiple policy assignments can be made for a given action. Matching actions are applied in sequence number order. If a respond or block action policy matches a request, ownership of the request is given to that policy and the policy selection is halted. If a modify policy matches a request, the policy is applied and policy selection continues.

For more information about configuring SIP HMR, refer to the *HMR Command Set on page 4762*. For additional SIP HMR and HMR intercept configuration information and examples, refer to the configuration guide *Manipulating SIP Headers and Messages in AOS*, available online at https://supportcommunity.adtran.com.

To enter the HMR Intercept Configuration mode, enter the **hmr intercept** command from the Global Configuration mode as follows:

```
(config)#hmr intercept
(config-hmr-intercept)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81

The commands available in the HMR Intercept Configuration mode are listed in alphabetical order below:

block <*policy name*>

Use the **block** <*policy name*> command to specify a header manipulation rules (HMR) intercept block action. Use the **no** form of this command to remove the block action from the HMR intercept configuration. Variations of this command include:

block <*policy name*>
block <*policy name*> <*sequence number*>

Syntax Description

<*policy name*>	Specifies the name of the block action policy.
<*sequence number*>	Optional. Specifies the sequence number given to the policy, which determines the order in which the policy actions are processed. Valid sequence number range is **1** to **99999**. If no sequence number is specified, a sequence number is automatically assigned so that new actions are placed at the end of the list of configured actions.

Default Values

By default, no HMR intercept block policies are configured.

Command History

Release 12.4.0	Command was introduced.

Functional Notes

Block action policies accept matching Session Initiation Protocol (SIP) requests and terminate those requests without generating a response. The rule set for this type of policy should include a message-rule of the **request** type that contains the necessary match rules to match the inbound request. No other rules are necessary because matching causes the request to be ignored.

If any changes are made to an HMR intercept policy, the HMR feature must be shutdown and restarted, using the command *shut on page 4820*, before the changes take effect.

Usage Examples

The following example configures an HMR rule set, **BlockOtherRegisters**, an HMR policy **BlockOtherRegisters** that applies the rule set, and also creates an HMR intercept policy that blocks SIP requests that match the **BlockOtherRegisters** rule set:

(config)**#hmr rule-set BlockOtherRegisters**
(config-rule-set-BlockOtherRegisters)**#message-rule MatchBlock message-type request 10**
(config-msg-rule-MatchBlock)**#match header sip-req-uri match-value REGISTER**
(config-msg-rule-MatchBlock)**#exit**
(config-rule-set-BlockOtherRegisters)**#exit**
(config)**#hmr policy BlockOtherRegisters**
(config-policy-BlockOtherRegisters)**#rule-set BlockOtherRegisters 10**
(config-policy-BlockOtherRegisters)**#exit**

(config)**#hmr intercept**
(config-hmr-intercept)**#block BlockOtherRegisters 30**
(config-hmr-intercept)**#no shut**

modify *<policy name>*

Use the **modify** *<policy name>* command to specify a header manipulation rules (HMR) intercept modify action. Use the **no** form of this command to remove the modify action from the HMR intercept configuration. Variations of this command include:

modify *<policy name>*
modify *<policy name>* *<sequence number>*

Syntax Description

<policy name>	Specifies the name of the modify action policy.
<sequence number>	Optional. Specifies the sequence number given to the policy, which determines the order in which the policy actions are processed. Valid sequence number range is **1** to **99999**. If no sequence number is specified, a sequence number is automatically assigned so that new actions are placed at the end of the list of configured actions.

Default Values

By default, no HMR intercept modify policies are configured.

Command History

Release 12.4.0	Command was introduced.

Functional Notes

Modify action policies apply the rules included in the policy to Session Initiation Protocol (SIP) requests. The rule set for this type of policy should include a message-rule of the **request** type that contains the necessary match rules to match the inbound request as well as the HMR rules necessary to modify the message as needed.

If any changes are made to an HMR intercept policy, the HMR feature must be shutdown and restarted, using the command *shut on page 4820*, before the changes take effect.

Usage Examples

The following example configures an HMR rule set, **ModifyNotify**, an HMR policy **ModifyNotify** that applies the rule set, and also creates an HMR intercept policy that modifies SIP requests that match the **ModifyNotify** rule set:

(config)**#hmr rule-set ModifyNotify**
(config-rule-set-ModifyNotify)**#message-rule ModifyNotify message-type request 10**
(config-msg-rule-ModifyNotify)**#match header sip-req-uri match-value NOTIFY**
(config-msg-rule-ModifyNotify)**#add header MyHeader position first new-value “New Header” 10**
(config-msg-rule-ModifyNotify)**#exit**
(config-rule-set-ModifyNotify)**#exit**
(config)**#hmr policy ModifyNotify**
(config-policy-ModifyNotify)**#rule-set ModifyNotify 10**

(config-policy-ModifyNotify)**#exit**
(config)**#hmr intercept**
(config-hmr-intercept)**#modify ModifyNotify 40**
(config-hmr-intercept)**#no shut**

respond <*policy name*>

Use the **respond** <*policy name*> command to specify a header manipulation rules (HMR) intercept response action. Use the **no** form of this command to remove the response action from the HMR intercept configuration. Variations of this command include:

respond <*policy name*>
respond <*policy name*> <*sequence number*>
respond <*policy name*> **code** <*response code*>
respond <*policy name*> **code** <*response code*> <*sequence number*>
respond <*policy name*> **code** <*response code*> **text** <*"response text"*>
respond <*policy name*> **code** <*response code*> **text** <*"response text"*> <*sequence number*>
respond <*policy name*> **text** <*"response text"*>
respond <*policy name*> **text** <*"response text"*> <*sequence number*>

Syntax Description

<*policy name*>	Specifies the name of the respond action policy.
<*sequence number*>	Optional. Specifies the sequence number given to the policy, which determines the order in which the policy actions are processed. Valid sequence number range is **1** to **99999**. If no sequence number is specified, a sequence number is automatically assigned so that new actions are placed at the end of the list of configured actions.
code <*response code*>	Optional. Specifies a response code to be used in the generated response. Valid range is **1** to **999**.
text <*"response text"*>	Optional. Specifies a response text to be used in the generated response. Enter response text in quotations.

Default Values

By default, no HMR intercept respond policies are configured. When respond policies are configured, if no response code is specified, by default a response code of **200** is used.

Command History

Release 12.4.0	Command was introduced.

Functional Notes

Respond action policies accept Session Initiation Protocol (SIP) requests that match the rules of the policy and send an appropriate response. The configuration of the respond action can include both response code and response text. The generated response can be modified by applicable rules included in the policy. The rule set for this type of policy should include a message-rule of the **request** type that contains the necessary match rules to match the inbound request. A second message-rule can be included if modification of the generated response is necessary.

If any changes are made to an HMR intercept policy, the HMR feature must be shutdown and restarted, using the command *shut on page 4820*, before the changes take effect.

Usage Examples

The following example configures an HMR rule set, **RespondToRegisterFromChicago**, an HMR policy **RespondToRegisterFromChicago** that applies the rule set, and also creates an HMR intercept policy that responds to SIP requests that match the **RespondToRegisterFromChicago** rule set:

(config)**#hmr rule-set RespondToRegisterFromChicago**
(config-rule-set-RespondToRegisterFromChicago)**#message-rule MatchRegister message-type request 10**
(config-msg-rule-MatchRegister)**#match header sip-req-uri match-value REGISTER**
(config-msg-rule-MatchRegister)**#match header contact match-value PlantA**
(config-msg-rule-ModifyRegister)**#exit**
(config-rule-set-RespondToRegisterFromChicago)**#message-rule ModifyResponse message-type response 20**
(config-msg-rule-ModifyResponse)**#add header PlantHeader position first new-value “Plant A” 10**
(config-msg-rule-ModifyResponse)**#exit**
(config-rule-set-RespondToRegisterFromChicago)**#exit**
(config)**#hmr policy RespondToRegisterFromChicago**
(config-policy-RespondToRegisterFromChicago)**#rule-set RespondToRegisterFromChicago 10**
(config-policy-RespondToRegisterFromChicago)**#exit**
(config)**#hmr intercept**
(config-hmr-intercept)**#respond RespondToRegisterFromChicago code 200 10**
(config-hmr-intercept)**#no shut**

shut

Use the **shut** command to disable the header manipulation rules (HMR) intercept feature. Use the **no** form of this command to enable the policy.

Syntax Description

No subcommands.

Default Values

By default, the HMR intercept policy is not active.

Command History

Release 12.4.0	Command was introduced.

Functional Notes

Any time an HMR intercept policy is modified, it must be shut down and then re-enabled for the changes to take effect.

Usage Examples

The following example enables the HMR intercept policy:

```
(config)#hmr intercept
(config-hmr-intercept)#no shut
```

MGCP COMMAND SET

Media Gateway Control Protocol (MGCP) is a protocol that works hand-in-hand with H.323 and Session Initiation Protocol (SIP) in Voice over Internet Protocol (VoIP) services. MGCP works between a call agent or media gateway controller, usually a software switch, and a media gateway with internal endpoints. The call agents create and manage media sessions with endpoints of physical or virtual data sources through the media gateway. The media gateway is the network device that converts voice signals carried by telephone lines into data packets carried over the Internet or other packet networks. In this network structure, AOS products function as a media gateway.

To enable MGCP functionality, enter the **ip mgcp** command from the Global Configuration mode prompt as follows:

```
>enable
#configure terminal
(config)#ip mgcp
(config)#
```

MGCP gateways communicate with internal MGCP endpoints. MGCP endpoints are dedicated foreign exchange station (FXS) ports configured to use MGCP to communicate with a call agent. The endpoints are configured with a few specialized MGCP commands and a large number of commands that are similar to those used for voice user configuration.

To create an MGCP endpoint and access its configuration, enter the **voice mgcp-endpoint** <*index*> command from the Global Configuration mode prompt as follows:

```
>enable
#configure terminal
(config)#voice mgcp-endpoint 1
(config-mgcp-1)#
```

The following configuration command set describes commands associated with configuring MGCP endpoints. For more information about MGCP gateway and endpoint configuration, refer to the *MGCP in AOS* configuration guide available online at https://supportcommunity.adtran.com.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83
interface on page 84

All other commands in this command set are described in this section in alphabetical order:

alc

Use the **alc** command to enable automatic level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature. Variations of this command include:

alc
alc level -16
alc level -17
alc level -18
alc level -19
alc level -20
alc level -21
alc level -22

Syntax Description

level -16	Optional. Specifies the ALC attenuation level is -16 dBm0.
level -17	Optional. Specifies the ALC attenuation level is -17 dBm0.
level -18	Optional. Specifies the ALC attenuation level is -18 dBm0.
level -19	Optional. Specifies the ALC attenuation level is -19 dBm0.
level -20	Optional. Specifies the ALC attenuation level is -20 dBm0.
level -21	Optional. Specifies the ALC attenuation level is -21 dBm0.
level -22	Optional. Specifies the ALC attenuation level is -22 dBm0.

Default Values

By default, ALC is disabled.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.
Release A2.04	Command was expanded to include the **level** parameters.

Usage Examples

The following example activates the ALC for MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#alc**

block-caller-id

Use the **block-caller-id** command to block caller ID information included in Media Gateway Control Protocol (MGCP) signaling on the endpoint. Use the **no** form of this command to allow caller ID information to appear.

Syntax Description

No subcommands.

Default Values

By default, caller ID information is allowed.

Command History

Release 10.1	Command was introduced.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example enables caller ID information blocking on MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#block-caller-id**

codec-group *<name>*

Use the **codec-group** command to specify the coder-decoder (CODEC) list to be used by this account. Use the **no** form of this command to remove the CODEC list from the account.

Syntax Description

<name>	Specifies the CODEC list to be used for this account.

Default Values

By default, no CODEC lists are assigned.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the integrated services digital network (ISDN) trunk.
Release 15.1	Command was added to the Voice Line Configuration command set.
Release A1	Command was included in the Voice Loopback Account Configuration command set.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) Configuration command set.

Functional Notes

The **codec-group** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation, and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893.*

Usage Examples

The following example applies the CODEC list **List1** to the MGCP endpoint **1**:

```
(config)#voice mgcp-endpoint 1
(config-mgcp-1)#codec-group List1
```


connect fxs <*slot/port*>

Use the **connect fxs** command to connect a Media Gateway Control Protocol (MGCP) endpoint to a physical foreign exchange station (FXS) port. Use the **no** form of this command to disconnect from the physical FXS port.

Syntax Description

<*slot/port*>	Specifies the slot and port to which the MGCP endpoint will connect. Slots and ports are entered as follows: **0/1**.

Default Values

By default, the endpoint is not connected to a physical port.

Command History

Release A2	Command was introduced.

Functional Notes

This command fails if the specified FXS port is already in use on another MGCP endpoint or by a configured voice user.

Usage Examples

The following example connects MGCP endpoint **1** to the physical FXS port **0/1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#connect fxs 0/1**

description *<text>*

Use the **description** command to give a textual description to a Media Gateway Control Protocol (MGCP) endpoint. Use the **no** form of this command to remove the endpoint's description.

Syntax Description

<text>	Specifies the textual description of the endpoint.

Default Values

By default, no description is given to an endpoint.

Command History

Release A2	Command was introduced.

Usage Examples

The following example gives the description of **farendpoint** to MGCP endpoint **1**:

(config)**#voice mgcp-endpoint1**
(config-mgcp-1)**#description farendpoint**

echo-cancellation

Use the **echo-cancellation** command to improve voice quality for packetized-based voice calls, such as Voice over Internet Protocol (VoIP) or Media Gateway Control Protocol (MGCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **echo-cancellation** is enabled.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example activates **echo-cancellation** for MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#echo-cancellation**

forward-disconnect delay

Use the **forward-disconnect delay** command to modify the forward disconnect delay time (in milliseconds) for the Media Gateway Control Protocol (MGCP) endpoint. Use the **no** form of this command to return the delay period to the default value. Variations of this command include:

forward-disconnect delay 250
forward-disconnect delay 500
forward-disconnect delay 750
forward-disconnect delay 900
forward-disconnect delay 1000
forward-disconnect delay 2000
forward-disconnect delay follow-switch

Syntax Description

250	Specifies a 250 ms delay time.
500	Specifies a 500 ms delay time.
750	Specifies a 750 ms delay time.
900	Specifies a 900 ms delay time.
1000	Specifies a 1000 ms delay time.
2000	Specifies a 2000 ms delay time.
follow-switch	Specifies a delay time follows the switch.

Default Values

By default, the forward disconnect delay is set to follow the switch.

Command History

Release A2.04	Command was introduced.
Release A4.01	Command syntax was updated from **fwd-disconnect delay** to **forward-disconnect delay**.

Functional Notes

Although the MGCP endpoint forward disconnect delay is set to follow the switch by default, this delay time varies depending on the endpoint's RFC 2833 signaling specification. If the RFC 2833 signaling is enabled, then the **follow-switch** parameter indicates that the Class 5 switch determines the length of the delay time. If RFC 2833 signaling is disabled, then using **follow-switch** indicates that the battery is removed for the default time of **900** ms.

Usage Examples

The following example specifies the forward disconnect delay for MGCP endpoint **1** is **1000** ms:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)#forward-disconnect delay 1000

modem-passthrough

Use the **modem-passthrough** command to switch to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings, such as echo cancellation and voice activity detection (VAD). Use the **no** form of this command to disable this feature. Variations of this command include:

modem-passthrough
modem-passthrough detection-time <*time*>
modem-passthrough cng-early-detect

Syntax Description

detection-time <*value*>	Optional. Specifies the fax and/or modem detection time length value in seconds. Range is **0** to **8** seconds.
cng-early-detect	Optional. Enables early (first burst) detection of fax calling (CNG) tone.

Default Values

By default, **modem-passthrough** is disabled. By default, the detection time is set to **8** seconds.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command was expanded.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.
Release A4.02	Command was expanded to include the **detection-time** parameter.
Release R10.8.0	Command was expanded to include the **cng-early-detect** parameter.

Usage Examples

The following example disables **modem-passthrough** on MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#no modem-passthrough**

name *<text>*

Use the **name** command to specify a textual name that the Media Gateway Control Protocol (MGCP) call agent will use to refer to a specific endpoint. Use the **no** form of this command to return to the default naming convention.

Syntax Description

<text>	Specifies the textual name of the MGCP endpoint.

Default Values

By default, when endpoints are created and given an index number, they are named in the following format: **aaln/x**, where **x** is the index number. For example, an endpoint with an index of **4** will by default have the name **aaln/4**.

Command History

Release A2	Command was introduced.

Usage Examples

The following example renames endpoint **1** as **endpoint243**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#name endpoint243**

nls

Use the **nls** command to enable the non-linear suppression (NLS) for the Media Gateway Control Protocol (MGCP) endpoint. This option is a component of echo cancellation. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example enables NLS for MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#nls**

plc

Use the **plc** command to enable packet loss concealment (PLC). PLC is used to attempt to mask lost or delayed packets by replacing the lost packet with another voice packet in the data stream. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, PLC is disabled.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.

Usage Examples

The following example disables PLC for the MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#no plc**

rtp delay-mode

Use the **rtp delay-mode** command to configure the Realtime Transport Protocol (RTP) jitter buffer mode settings. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Use the **no** form of this command to return to the default setting. Variations of this command include:

rtp delay-mode adaptive
rtp delay-mode fixed

Syntax Description

adaptive	Configures the RTP jitter buffer packet delay to adjust during a call based on network conditions.
fixed	Configures the RTP jitter buffer packet delay to remain constant.

Default Values

By default, the RTP delay mode is set to **adaptive**. This allows for minimal latency by adjusting the average packet delay based on the conditions of the network.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.

Usage Examples

The following example configures RTP delay mode as **fixed** on MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#rtp delay-mode fixed**

rtp dtmf-relay

Use the **rtp dtmf-relay** command to configure the method by which Realtime Transport Protocol (RTP) dual tone multi-frequency (DTMF) events are relayed. The dial digits can be sent inband or out-of-band (OOB) of the voice stream. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp dtmf-relay inband
rtp dtmf-relay nte <*value*>

Syntax Description

inband	Specifies that RTP DTMF events be relayed inband in the RTP stream.
nte <*value*>	Specifies that RTP DTMF events be relayed OOB using named telephone events (NTEs). Enter an NTE value between **96** and **127**.

Default Values

By default, the **rtp dtmf-relay** is set for **NTE 101**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.

Usage Examples

The following example configures RTP DTMF relay events for **inband**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#rtp dtmf-relay inband**

rtp frame-packetization <*value*>

Use the **rtp frame-packetization** command to configure the Realtime Transport Protocol (RTP) frame packetization time in milliseconds for individual Media Gateway Control Protocol (MGCP) endpoints. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP frame packetization time value in milliseconds. Select from **10**, **20**, or **30** milliseconds.

Default Values

By default, the **rtp frame-packetization** time is set to **20** milliseconds on all MGCP endpoints.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example sets the frame packetization time for MGCP endpoint **1** to **10** milliseconds:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#rtp frame-packetization 10**

rtp packet-delay

Use the **rtp packet-delay** command to configure the maximum Realtime Transport Protocol (RTP) packet delays. This command is used to set the allowable limits of latency on the network. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp packet-delay fax <*value*>
rtp packet-delay maximum <*value*>
rtp packet-delay nominal <*value*>

Syntax Description

fax <*value*>	Sets the fax delay time value in increments of **10** milliseconds. Range is **0** to **500** milliseconds.
maximum <*value*>	Sets the maximum delay time value in increments of **10** milliseconds. Range is **40** to **320** milliseconds.
nominal <*value*>	Sets the nominal delay time value in increments of **10** milliseconds. Range is **10** to **240** milliseconds.

Default Values

By default, the RTP packet delay for fax is **50**, maximum is **100**, and for nominal is **50**.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.

Usage Examples

The following example configures the RTP maximum delay time on MGCP endpoint **1** to **200** milliseconds:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#rtp packet-delay maximum 200**

rtp qos dscp <*value*>

Use the **rtp qos dscp** command to configure the maximum Realtime Transport Protocol (RTP) quality of service (QoS) parameters for differentiated services code point (DSCP). Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP QoS parameter for DSCP. Enter a value between **10** and **63**.

Default Values

By default, the RTP QoS parameter for DSCP on Media Gateway Control Protocol (MGCP) endpoints is **46**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example configures the RTP QoS DSCP for MGCP endpoint **1** to **60**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#rtp qos dscp 60**

t38

Use the **t38** command to enable T.38 fax operation on the Media Gateway Control Protocol (MGCP) endpoint. Use the **no** form of this command to disable this feature.

*The **modem-passthrough** command must be enabled for T.38 operation to work. Refer to modem-passthrough on page 4830 for more information.*

Syntax Description

No subcommands.

Default Values

By default, T.38 is disabled.

Command History

Release 16.1	Command was introduced.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example enables T.38 on MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38**

Technology Review

T.38 is an International Telecommunication Union (ITU) specification that allows Group-3 Fax (T.30) data to be transported over the Internet. It is similar to dual tone multi-frequency (DTMF) relay (RFC 2833) in that the digital signal processor (DSP) decodes tones and demodulated fax data and converts them into packets. A similar device on the other end takes the packets/tones and remodulates them so that an analog fax machine on the other end can receive the fax. AOS's previous support (revisions 12 through 15) for fax/modem signals was simply detecting a tone and forcing the coder-decoder (CODEC) into G.711 and disabling/enabling echo cancellers based on the tones detected. When packet loss becomes high, sending faxes over G.711 becomes problematic, due to dropped messages and timeouts/retrains.

T.38 can be used in conjunction with various call-control schemes, such as H.323, Session Initiation Protocol (SIP), and MGCP. AOS only supports SIP as the call-control method. This is typically referred to T.38/Annex-D. Annex-D describes the Session Initiation Protocol/Session Description Protocol (SIP/SDP) call establishment procedures.

t38 ced auto-generate

Use the **t38 ced auto-generate** command to specify when the digital signal processor (DSP) should regenerate the called station identifier (CED) signal toward the time division multiplexed (TDM) endpoint. If auto-generate is enabled, the DSP generates the CED signal only when it does not receive CED indicator packets from the Voice over IP (VoIP) endpoint. If auto-generate is disabled, the DSP generates the CED signal only when it does receive CED indicator packets from the VoIP endpoint. Using the **no** version of this command disables CED auto-generate.

Syntax Description

No subcommands.

Default Values

By default, CED auto-generate is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example enables CED auto-generate for the T.38 session on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 ced auto-generate**

t38 ced length <*time*>

Use the **t38 ced length** command to set the maximum duration of a regenerated called station identifier (CED) signal, in milliseconds, from the digital signal processor (DSP) toward the time division multiplexed (TDM) endpoint when a T.38 session is active. Using the **no** form of this command returns the duration to the default value.

Syntax Description

<*time*>	Specifies the maximum duration of a regenerated CED signal in milliseconds. Valid range is **0** to **4000** ms.

Default Values

By default, the maximum duration of a regenerated CED signal is **3000** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Setting the maximum duration of a regenerated CED signal to **0** effectively prevents any CED generation.

Usage Examples

The following example decreases the maximum duration of the CED signal to **2000** ms for the T.38 session on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 ced length 2000**

t38 cng-relay-selective

Use the **t38 cng-relay-selective** command to enable fax calling tones (CNG) relay only when V.21 messages are not being transmitted. Use the **no** version of this command to disable selective CNG relay.

Syntax Description

No subcommands.

Default Values

Selective CNG relay is disabled by default.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables T.38 CNG relay:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 cng-relay-selective**

t38 ecm

Use the **t38 ecm** command to enable or disable error correction mode (ECM) during T.38 sessions. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 ecm enable
t38 ecm disable

Syntax Description

enable	Enables ECM during T.38 sessions.
disable	Disables ECM during T.38 sessions.

Default Values

By default, ECM is enabled.

Command History

Release R10.8.0	The command was introduced

Usage Examples

The following example disables ECM for T.38 sessions on MGCP endpoint 1:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 ecm disable**

t38 error-correction

Use the **t38 error-correction** command to specify the type of fax error correction. Use the **no** form of this command to disable this feature. Variations of this command include:

t38 error-correction fec
t38 error-correction redundancy

Syntax Description

fec	Specifies forward error correction (FEC) as the fax error correction. FEC is a system of error control where the sender adds redundant data to its messages, allowing the receiver to detect and correct errors (within certain bounds) without the need to request additional data from the sender.
redundancy	Specifies redundancy as the fax error correction. Redundancy error correction replicates the payload a user-specified number of times to determine if errors are present. The number of redundant packets is set using the command *t38 v21-preamble-timeout <value> on page 4851*).

Default Values

By default, **t38 error-correction** is set to **redundancy** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, the NetVanta 6240/6250 Serires, and the NetVanta 640 Series.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default value changed to **fec** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 6355 Series products.
Release R10.8.0	The default values for this command were updated.

Usage Examples

The following example sets the **t38 error-correction** to **fec** for the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 error-correction fec**

t38 fallback-mode g711

Use the **t38 fallback-mode** command to specify the transmission mode used when T.38 fax relay cannot be successfully negotiated at the time of the fax transfer. Use the **no** form of this command to disable this feature.

Syntax Description

g711	Specifies that fax operation revert back to analog mode (G.711).

Default Values

By default, **t38 fallback-mode** is to **G.711**.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **G.711**.

Usage Examples

The following example enables the **t38 fallback-mode** on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 fallback-mode g711**

t38 generate-cng

Use the **t38 generate-cng** command to specify whether the digital signal processor (DSP) will begin a T.38 session by generating the calling signal (CNG) toward the time division multiplexed (TDM) endpoint. Using the **no** version of this command disables CNG generation.

Syntax Description

No subcommands.

Default Values

By default, CNG generation is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

With the introduction of this command, the CNG generation behavior of the T.38 session is now configurable. In AOS firmware prior to A5.01, this behavior was not configurable, but rather was set to always generate this signal.

Usage Examples

The following example enables CNG generation for the T.38 session on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 generate-cng**

t38 max-buffer <*value*>

Use the **t38 max-buffer** command to set the maximum buffer size for T.38 fax operation. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-buffer** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **800** bytes.

Default Values

By default, the maximum buffer size is set to **200**.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-buffer** to **100** on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 max-buffer 100**

t38 max-datagram <*value*>

Use the **t38 max-datagram** command to set the maximum datagram value in this unit. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-datagram** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **300** bytes.

Default Values

By default, the maximum datagram value is set to **72** bytes.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **72** bytes.

Usage Examples

The following example sets the **t38 max-datagram** to **100** on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 max-datagram 100**

t38 max-rate

Use the **t38 max-rate** command to specify the fax maximum rate. The actual transmission rate could be lower than specified rate if the receiving end cannot support the maximum rate. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 max-rate 14400
t38 max-rate 12000
t38 max-rate 2400
t38 max-rate 4800
t38 max-rate 7200
t38 max-rate 9600

Syntax Description

14400	Specifies 14400 bits per second (bps) as fax maximum rate.
12000	Specifies 12000 bps as fax maximum rate.
2400	Specifies 2400 bps as fax maximum rate.
4800	Specifies 4800 bps as fax maximum rate.
7200	Specifies 7200 bps as fax maximum rate.
9600	Specifies 9600 bps as fax maximum rate.

Default Values

By default, the maximum fax rate is set to **14400** bps.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-rate** to **4800** bps on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 max-rate 4800**

t38 redundancy

Use the **t38 redundancy** command to set the number of redundant packets sent when the **t38 error-correction redundancy** feature is enabled on Media Gateway Control Protocol (MGCP) endpoints. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 redundancy high-speed <*value*>
t38 redundancy low-speed <*value*>

Syntax Description

high-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for data messages (high-speed fax machine image data). Range is **0** (no redundancy) to **4** packets.
low-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for the signaling messages (low-speed fax machine protocol). Range is **0** (no redundancy) to **7** packets.

Default Values

By default, high-speed and low-speed redundancy values are set to **0** (no redundancy).

Command History

Release 16.1	Command was introduced.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example enables **t38 error-correction redundancy** and sets the number of redundant data messages to **high-speed 3** on MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 error-correction redundancy**
(config-mgcp-1)**#t38 redundancy high-speed 3**

t38 v21-preamble-timeout *<value>*

Use the **t38 v21-preamble-timeout** command to set the maximum amount of time that the digital signal processor (DSP) waits for peer device activity after starting to transmit a V.21 preamble event before spoofing a response to the time division multiplexed (TDM) endpoint. Using the **no** version of this command returns the timeout value to the default setting.

Syntax Description

<value>	The time, in milliseconds, that the DSP will wait for peer activity. Valid range is **1** to **3000** ms.

Default Values

By default, the V.21 preamble timeout is set to **1700** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example specifies the V.21 preamble timeout value as **2000** ms on the Media Gateway Control Protocol (MGCP) endpoint:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#t38 v21-preamble-timeout 2000**

vad

Use the **vad** command to enable voice activity detection (VAD) on Media Gateway Control Protocol (MGCP) endpoints. VAD blocks out noise categorized as silence during a voice connection. The silent voice packets are not transmitted, allowing bandwidth usage to be reduced. Although VAD saves bandwidth, the quality of the voice call may be compromised. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, VAD is enabled for all MGCP endpoints.

Command History

Release 9.3	Command was introduced.
Release A2	Command was added to the MGCP endpoint configuration.

Usage Examples

The following example disables VAD on MGCP endpoint **1**:

(config)**#voice mgcp-endpoint 1**
(config-mgcp-1)**#no vad**

MUSIC ON HOLD COMMAND SET

Music on hold (MOH) is a feature that allows the user to play hold music internally from a NetVanta 7000 Series unit rather than using an external music player. This feature replaces the CD player or other hardware that would normally be required to generate hold music. The MOH feature can be used for hold music, as well as for call queues and FindMe-FollowMe.

For more information about configuring MOH, refer to the quick configuration guide *Configuring Music on Hold on the NetVanta 7000 Series* available online at https://supportcommunity.adtran.com.

To specify a MOH player and enter the Voice Music on Hold Configuration mode, enter the **voice music-on-hold player** <*name*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice music-on-hold player moh1
(config-moh1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

cross-connect on page 76
do on page 81
exit on page 83

All other commands for this command set are described in this section in alphabetical order:

default on page 4854
file <filename> on page 4855

default

Use the **default** command to set the current music on hold (MOH) player as the default player. Use the **no** version of this command to restore the system default.

Default Values

By default, the **system** player is set as the default player.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the player **MOH1** as the default MOH player:

```
(config)#voice music-on-hold player MOH1
(config-moh1)#default
```

file <*filename*>

Use the **file** command to add music files to a music on hold (MOH) player. Use the **no** version of this command to remove the file from the MOH player.

Syntax Description

<*filename*>	Specifies the name of the music file to be added to the MOH player.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example adds the file named **holdmusic1.wav** to the MOH player:

(config)**#voice music-on-hold player moh1**
(config-moh1)**#file holdmusic1.wav**

PROXY USER TEMPLATE COMMAND SET

The proxy user template is an expanded function of the Session Initiation Protocol (SIP) Proxy feature on Adtran Operating System (AOS) products. By creating a proxy user template on the AOS device serving as a SIP Proxy, calls are allowed to route to a private branch exchange (PBX) even if the SIP Proxy has not received a REGISTER request from that user on the PBX. Users are dynamically added to the proxy user database when an INVITE or SUBSCRIBE message is received from the user, allowing SIP messages to be routed for the identified user. The user template makes it possible to route traffic for users not already known by the SIP Proxy. This feature can also direct certain calls to local external public switch telephone network (PSTN) gateways.

The commands in this section help you to create and define a template, as well as explain how calls received by the SIP Proxy respond to these configuration parameters. For more information about SIP Proxy configuration, refer to the configuration guide *Configuring SIP Proxy in AOS* available online at https://supportcommunity.adtran.com.

To create a proxy user template and enter the proxy user template configuration mode, enter the **sip proxy user-template** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#sip proxy user-template Set1
(config-template-Set1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

accept <template> on page 4857
expire-time <seconds> on page 4859
match on page 4860
proxy-mode on page 4861
reject <template> on page 4862
routeback-rejection on page 4864
target <host> on page 4865

accept *<template>*

Use the **accept** command to specify a number pattern to match to a user ID and add the user to the Session Initiation Protocol (SIP) Proxy user database. Once the **accept** entry is added to the proxy user template, SIP messages are permitted and routed on the proxy server for the identified user. Use the **no** form of this command to remove a configured template entry from the proxy user template.

*AOS will process the **reject** patterns before the **accept** patterns, regardless of the order they appear in the configuration of the proxy user template. Refer to reject <template> on page 4862 for additional information.*

Syntax Description

<template>	Specifies the patterns to match to a proxy user and allow the user as an entry to the SIP Proxy user database. You can enter a complete phone number, or use wildcards to define accepted numbers. Refer to *Functional Notes* below for more information on using wildcards.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example configures the **Set1** proxy user template to permit SIP messages for users with the 256-555 exchange in their ID:

(config)**#sip proxy user-template Set1**
(config-template-Set1)**#accept 256555XXXX**

expire-time *<seconds>*

Use the **expire-time** command to set the number of seconds before a proxy user entry is removed from the SIP proxy user database. In the Proxy User Template command set, this command applies to a user entry created as a result of matching the specified proxy user template. Use the **no** form of this command to return to the default value of **3600** seconds.

Syntax Description

<seconds>	Specifies the number of seconds until the user entry expires. Valid range is **30** to **86400** seconds. A value of **0** means the entry will never expire.

Default Values

By default, the expiration time is set to **3600**, which means the user entry will be removed from the database after 1 hour.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example sets the expiration time to **7200** seconds (or 2 hours) for the **Set1** proxy user template:

(config)**#sip proxy user-template Set1**
(config-template-Set1)**#expire-time 7200**

match

Use the **match** command to configure the proxy user template match settings for specific traffic patterns. Use the **no** form of this command to disable a match setting. Variations of this command include:

match inbound
match outbound
match outbound source contact
match outbound source from
match outbound source from enable-alternate-identity

Syntax Description

inbound	Specifies that this proxy user template should be used to match against inbound traffic.
outbound	Specifies that this proxy user template should be used to match against outbound traffic.
source	Specifies the Session Initiation Protocol (SIP) header type(s) to use when matching the proxy user template against outbound traffic.
contact	Specifies that the Contact header should be used when matching the proxy user template against outbound traffic.
from	Specifies that the From header should be used when matching the proxy user template against outbound traffic.
enable-alternate-identity	Specifies that the P-Preferred-Indentity, P-Asserted-Identity or Remote-Party-ID header, if present, should be used in place of the From header when matching the proxy user template against outbound traffic.

Default Values

By default, the Contact header is used when matching the proxy user template agains outbound traffic.

Command History

Release A5.01	Command was introduced.

Functional Notes

For more information on the operation and configuration of SIP proxy, refer to the configuration guide *Configuring SIP Proxy in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the Set1 proxy user template should be used to match against outbound traffic and that the From header should be used:

(config)**#sip proxy user-template Set1**
(config-template-Set1)**#match outbound source from**

proxy-mode

Use the **proxy-mode** command to enable the appropriate Session Initiation Protocol (SIP) proxy operation mode for users added to the SIP proxy user database by the specified proxy user template. Use the **no** form of this command to return to the default setting. Variations of this command include:

proxy-mode auto
proxy-mode outbound-proxy
proxy-mode stateful
proxy-mode transparent

Syntax Description

auto	Detects the correct proxy mode automatically.
outbound-proxy	Specifies using outbound proxy mode.
stateful	Specifies using stateful proxy mode.
transparent	Specifies using transparent proxy mode.

Default Values

By default, this feature is set to **auto**. The **auto** setting detects the correct proxy mode for outbound requests based upon how the INVITE is addressed. The correct proxy mode for inbound requests cannot be initially detected until the proxy server has trained using an outbound message from the user. Therefore, in situations where it is essential to correctly identify the proxy mode for inbound messages, it is suggested to specifically configure the **proxy-mode** for **outbound-proxy**, **stateful**, or **transparent**, whichever is most appropriate for your situation.

Command History

Release A4.01	Command was introduced.

Functional Notes

For more information on the operation and configuration of SIP proxy, refer to the configuration guide *Configuring SIP Proxy in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables transparent proxy mode operation for users added by the **Set1** proxy user template:

(config)**#sip proxy user-template Set1**
(config-template-Set1)**#proxy-mode transparent**

reject *<template>*

Use the **reject** command to specify a number pattern to match to a user ID for rejection from the SIP Proxy user database. If a match is successful, SIP messages are rejected for the matching user. Use the **no** form of this command to remove a configured template entry from the proxy user template.

> NOTE *AOS will process the **reject** patterns before the **accept** patterns, regardless of the order they appear in the configuration of the proxy user template. Refer to accept <template> on page 4857 for additional information.*

Syntax Description

<template>	Specifies the patterns to match a proxy user and reject the user as an entry to the SIP proxy user database. You can enter a complete phone number, or wildcards can be used to help define rejected numbers. Refer to *Functional Notes* below for more information on using wildcards.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.

2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example configures the **Set1** proxy user template to reject the user matching ID **2565556031** as an entry to the SIP proxy user database:

(config)**#sip proxy user-template Set1**
(config-template-Set1)**#reject 2565556031**

routeback-rejection

Use the routeback-rejection command to specify that during failover the proxy user template should not be used if the Contact header matches the template's target. Use the **no** form of this command to disable routeback rejection.

Syntax Description

No subcommands.

Default Values

By default, routeback-rejection is disabled.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example enables routeback rejection for proxy user template **Set1**:

(config)**#sip proxy user-template Set1**
(config-template-Set1)**#routeback-rejection**

target <*host*>

Use the **target** command to specify the proxy user's location. This command indicates the host name or IP address, protocol, and port number to use in locating the proxy user. Use the **no** form of this command to remove the target configuration. Variations of this command include:

target <*host*>
target <*host*> **tcp**
target <*host*> **tcp** <*port*>
target <*host*> **udp**
target <*host*> **udp** <*port*>

Syntax Description

<*host*>	Specifies the fully qualified domain name (FQDN) or IP address of the target server. IP addresses should be expressed in dotted decimal notation (for example, 208.61.209.1).
tcp	Optional. Specifies using Transmission Control Protocol (TCP).
udp	Optional. Specifies using User Datagram Protocol (UDP).
<*port*>	Optional. Specifies the TCP or UDP port used by the target host. Range is **1** to **65535**.

Default Values

By default, no target server is configured. If a target is configured with no protocol or port specified, the proxy server operates using UDP on port **5060**. If a protocol is specified, but no port is specified, the proxy server uses port **5060**.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies the users matching the proxy user template **Set1** are located at IP address **10.10.10.3** and to use UDP port **5061**:

(config)**#sip proxy user-template Set1**
(config-template-Set1)**#target 10.10.10.3 udp 5061**

SIP PROXY MONITOR COMMAND SET

The Session Initiation Protocol (SIP) proxy monitor feature provides support for monitored rollover to the SIP proxy in stateful mode. When the currently selected SIP server is unresponsive, the proxy uses a secondary proxy server for future calls. In the event the selected secondary SIP server becomes unresponsive, the proxy will roll over to the next available secondary server. As more preferred servers are returned to service, all future calls are routed to it.

When enabled, the SIP proxy monitor can operate in one of two modes: **continuous** or **on-failure**. In continuous mode, the proxy monitor continues to poll the currently selected SIP proxy server to determine its operational state. In contrast, the on-failure mode only polls SIP proxy servers during a detected failure state. The mode is configured using the **mode** command in this command set.

Additional monitoring behaviors can be configured to specify the poll timeout, intervals, recover response, poll requests grammar, and SNMP traps. Each configuration option is explained in detail in this command set.

For more information about SIP proxy implementation and configuration in AOS, refer to the configuration guide *Configuring SIP Proxy in AOS*, available online at http://supportforums.adtran.com.

To enable the SIP proxy SIP server monitor, and enter the SIP proxy SIP server monitor configuration mode, enter the following command from the Global Configuration mode:

```
(config)#sip proxy sip-server monitor
    Configuring New Proxy Monitor.
(config-proxy-monitor)#
```

Once you have entered the SIP Proxy SIP Server Monitor Configuration mode, you can configure the specific behavior of the proxy monitor feature.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

grammar from user on page 4867
grammar request-uri user on page 4868
grammar to user on page 4869
mode on page 4870
poll timeout <value> on page 4871
recover on page 4872
trap rollover on page 4874

grammar from user

Use the **grammar from user** command to configure the User field of the From header on Session Initiation Protocol (SIP) proxy monitor poll requests. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar from user none
grammar from user <*username*>

Syntax Description

none	Specifies the user is not included in the User field of the From header.
<*username*>	Specifies the user name used to format the User field of the From header.

Default Values

By default, the user is not specified in the From header. The default value is set to **none**.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example sets the User field for the From header to **2565555229**:

(config)**#sip proxy sip-server monitor**
Configuring New Proxy Monitor.
(config-proxy-monitor)**#grammar from user 2565555229**

grammar request-uri user

Use the **grammar request-uri user** command to configure the Request uniform resource identifier (URI) header user on Session Initiation Protocol (SIP) proxy monitor poll requests. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar request-uri user none
grammar request-uri user <*username*>

Syntax Description

none	Specifies the user is not included in the Request-URI header.
<*username*>	Specifies the user name used to format the User field of the Request-URI header.

Default Values

By default, the user is not specified in the Request-URI header. The default value is set to **none**.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example sets the User field for the Request-URI header to **none**:

(config)**#sip proxy sip-server monitor**
Configuring New Proxy Monitor.
(config-proxy-monitor)**#grammar request-uri user none**

grammar to user

Use the **grammar to user** command to configure the User field of the To header on Session Initiation Protocol (SIP) proxy monitor poll requests. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar to user none
grammar to user <*username*>

Syntax Description

none	Specifies the user is not included in the User field of the To header.
<*username*>	Specifies the user name used to format the User field of the To header.

Default Values

By default, the user is not specified in the To header. The default value is set to **none**.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example sets the User field for the To header to **2565555229**:

(config)**#sip proxy sip-server monitor**
Configuring New Proxy Monitor.
(config-proxy-monitor)**#grammar to user 2565555229**

mode

Use the **mode** command to configure the polling behavior of the Session Initiation Protocol (SIP) proxy monitor. Use the **no** form of this command to return to the default setting. Variations of this command include:

mode continuous
mode continuous interval <*value*>
mode on-failure

Syntax Description

continuous	Specifies proactive polling of the current SIP proxy server. Even if the SIP proxy monitor detects all servers are functioning, the SIP proxy monitor continues to poll them on a continuous basis.
interval <*value*>	Optional. Specifies the continuous polling interval. Valid range is **1** to **84600** seconds. The default value is **30** seconds.
on-failure	Specifies polling SIP proxy servers only when a failed state is detected. Once the server returns to a functioning state, the polling is ceased.

Default Values

By default, the SIP proxy monitor polling mode is set to poll **on-failure**.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example configures the SIP proxy monitor to poll SIP servers continuously at **1200** second intervals:

(config)**#sip proxy sip-server monitor**
Configuring New Proxy Monitor.
(config-proxy-monitor)**#mode continuous interval 1200**

poll timeout *<value>*

Use the **poll timeout** command to configure the poll request timeout for the Session Initiation Protocol (SIP) proxy monitor. This value defines the number of seconds the SIP proxy monitor must wait for a response when issuing poll requests to a SIP server. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the timeout value. Valid range is **1** to **600** seconds.

Default Values

By default, the poll requests are set to timeout after **32** seconds.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example configures the poll timeout to **16** seconds:

(config)**#sip proxy sip-server monitor**
Configuring New Proxy Monitor.
(config-proxy-monitor)**#poll timeout 16**

recover

Use the **recover** command to configure the polling behavior of the Session Initiation Protocol (SIP) proxy monitor. The recover interval only takes affect when the server is down. Use the **no** form of this command to return to the default setting. Variations of this command include:

recover delay <*min*>
recover delay <*min*> <*max*>
recover no-response interval <*value*>
recover no-response interval <*min*> <*max*>
recover responses <*value*> **interval** <*value*>

Syntax Description

delay	Configures the SIP proxy monitor recovery delay. In a failover situation, this delay allows the AOS device to delay communication attempts to a SIP proxy server for a specified amount of time.
<*min*>	Specifies the minimum recovery delay period. Valid range is **0** to **86400** seconds.
<*max*>	Specifies the maximum recover delay period. Valid range is **0** to **86400** seconds. The <*max*> value must be greater than the <*min*> value. When both values are configured, a random selection of the timeout value within the indicated range occurs.
no-response interval	Specifies proxy monitor recovery operation when no response is received from the SIP server.
<*value*>	Specifies the interval at which the proxy monitor will poll the SIP server. Valid range is **1** to **86400** seconds.
<*min*> <*max*>	Specifies a range for the interval at which the proxy monitor will poll the SIP server. Valid range is **1** to **86400** seconds. The first value is the minimum value which is the starting interval. The second value is the maximum value to which the interval works up. The interval time is doubled with each time the SIP server fails to respond until the maximum is reached, which is where the interval setting will stay.
responses	Specifies the number of successful responses necessary to recover service to the SIP server and the interval at which the polls are sent.
<*value*>	Specifies the number of successful responses needed to recover. Valid range is **1** to **255**.
interval <*value*>	Specifies the interval at which polls are sent after a successful response is received from the SIP server. Valid range is **1** to **86400** seconds.

Default Values

By default, the SIP proxy monitor is set to recover after **3** responses to polls sent at **10** second intervals. The **recover no-response interval** is set to a minimum of **5** and a maximum of **60**.

Command History

Release R10.9.0	Command was introduced.
Release R11.7.0	Command was expanded to include the **recover delay** parameter.

Usage Examples

The following example configures the SIP proxy SIP server monitor to recover after **7** successful responses are received at **32** second intervals:

(config)**#sip proxy sip-server monitor**
Configuring New Proxy Monitor.
(config-proxy-monitor)**#recover responses 7 interval 32**

The following example configures the SIP proxy SIP server monitor to send recover poll requests to the SIP server at 60 second intervals:
(config)**#sip proxy sip-server monitor**
Configuring New Proxy Monitor.
(config-proxy-monitor)**#recover no-response interval 60**

trap rollover

Use the **trap rollover** command to enable Simple Network Management Protocol (SNMP) traps when Session Initiation Protocol (SIP) proxy monitor rollover occurs. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the SNMP traps are disabled for SIP proxy SIP server monitor rollover.

Command History

Release R10.9.0	Command was introduced.

Usage Examples

The following example enables SNMP traps when the SIP proxy SIP server monitor rollover occurs:

```
(config)#sip proxy sip-server monitor
    Configuring New Proxy Monitor.
(config-proxy-monitor)#trap rollover
```

SIP SERVER MONITOR COMMAND SET

The Session Initiation Protocol (SIP) server monitor feature provides support for monitoring the availability of SIP servers for validated SIP trunk failover configurations. When the currently selected SIP server is unresponsive, the SIP server monitor causes the SIP trunk to use a secondary SIP server for future calls through a monitored rollover procedure. In the event the selected secondary SIP server becomes unresponsive, the SIP server monitor will then roll over to the next available secondary server. As a more preferred server is returned to service, all future calls are routed to it.

When enabled, the SIP server monitor can operate in one of two modes: **continuous** or **on-failure**. In continuous mode, the server monitor continues to poll the currently selected SIP server to determine its operational state. In contrast, the on-failure mode only polls SIP servers during a detected failure state. The mode is configured using the **mode** command in this command set.

Additional monitoring behaviors can be configured to specify the poll timeout, intervals, and recovery responses. Each configuration option is explained in detail in this command set.

For more information about SIP server monitor and validated SIP trunk failover configuration in AOS, refer to the configuration guide *Configuring SIP Trunk Failover in AOS*, available online at http://supportcommunity.adtran.com.

To enable the SIP server monitor, and enter the SIP Server Monitor configuration mode, enter the following command from the SIP Trunk Configuration mode:

```
(config)#voice trunk t01 type sip
(config-T01)#sip-server monitor
    Configuring SIP Server Monitor.
(config-sip-server-monitor)#
```

Once you have entered the SIP Server Monitor Configuration mode, you can configure the specific behavior of the SIP server monitor feature.

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

exit on page 83
shutdown on page 93

All other commands for this command set are described in this section in alphabetical order.

mode on page 4876
poll timeout <value> on page 4877
recover on page 4878

mode

Use the **mode** command to configure the polling behavior of the Session Initiation Protocol (SIP) server monitor. Use the **no** form of this command to return to the default setting. Variations of this command include:

mode continuous
mode continuous interval <*value*>
mode on-failure

Syntax Description

continuous	Specifies proactive polling of the current SIP server. Even if the SIP server monitor detects all servers are functioning, the SIP server monitor continues to poll them on a continuous basis.
interval <*value*>	Optional. Specifies the continuous polling interval. Valid range is **1** to **86400** seconds. The default value is **60** seconds.
on-failure	Specifies polling SIP servers only when a failed state is detected. Once the server returns to a functioning state, the polling is ceased.

Default Values

By default, the SIP server monitor polling mode is set to poll **on-failure**.

Command History

Release R13.11.0	Command was introduced.

Functional Notes

If the continuous polling interval is specified, it should not be less than 64 multiplied by the configured value of the SIP T1 timer (specified using the command *sip timer on page 1772*).

Usage Examples

The following example configures the SIP server monitor to poll SIP servers continuously at **1200** second intervals:

```
(config-T01)#sip-server monitor
    Configuring SIP Server Monitor.
(config-sip-server-monitor)#mode continuous interval 1200
```


poll timeout *<value>*

Use the **poll timeout** command to configure the poll request timeout for the Session Initiation Protocol (SIP) server monitor. This value defines the number of seconds the SIP server monitor must wait for a response when issuing poll requests to a SIP server. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the timeout value. Valid range is **1** to **600** seconds.

Default Values

By default, the poll requests are set to timeout after **32** seconds.

Command History

Release R13.11.0	Command was introduced.

Functional Notes

The **poll timeout** value should not be greater than 64 multiplied by the configured value of the SIP T1 timer (specified using the command *sip timer on page 1772*).

Usage Examples

The following example configures the poll timeout to **16** seconds:

```
(config-T01)#sip-server monitor
    Configuring SIP Server Monitor.
(config-sip-server-monitor)#poll timeout 16
```


recover

Use the **recover** command to configure the recovery polling behavior of the Session Initiation Protocol (SIP) server monitor. The recover interval only takes affect when the server is down. Use the **no** form of this command to return to the default setting. Variations of this command include:

recover delay <*min*>
recover delay <*min*> <*max*>
recover no-response interval <*value*>
recover no-response interval <*initial*> <*max*>
recover responses <*value*> **interval** <*value*>

Syntax Description

delay	Configures the SIP server monitor recovery delay. In a SIP trunk failover situation, this delay allows the AOS device to delay communication attempts to a SIP server for a specified amount of time.
<*min*>	Specifies the minimum recovery delay period. Valid range is **0** to **86400** seconds.
<*max*>	Optional. Specifies the maximum recover delay period. Valid range is **0** to **86400** seconds. The <*max*> value must be greater than the <*min*> value. When both values are configured, a random selection of the timeout value within the indicated range occurs.
no-response interval	Specifies SIP server monitor recovery operation when no response is received from the SIP server.
<*value*>	Specifies the interval at which the SIP server monitor will poll the SIP server. Valid range is **1** to **86400** seconds.
<*initial*> <*max*>	Specifies a range for the interval at which the SIP server monitor will poll the SIP server. Valid range is **1** to **86400** seconds. The first value is the initial value which is the starting interval. The second value is the maximum value to which the interval works up. The interval time is doubled with each time the SIP server fails to respond until the maximum is reached, which is where the interval setting will stay.
responses	Specifies the number of successful responses necessary to recover service to the SIP server and the interval at which the polls are sent.
<*value*>	Specifies the number of successful responses needed to recover. Valid range is **1** to **255**.
interval <*value*>	Specifies the interval at which polls are sent after a successful response is received from the SIP server. Valid range is **1** to **86400** seconds.

Default Values

By default, the SIP server monitor is set to recover after **3** responses to polls sent at **10** second intervals. The **recover no-response interval** is set to an initial interval of **5** and a maximum of **60**.

Command History

Release R10.9.0	Command was introduced.
Release R13.11.0	Command was expanded to include the **no-response** and **responses** parameters.

Usage Examples

The following example configures the SIP server monitor to recover after **7** successful responses are received at **32** second intervals:

```
(config-T01)#sip-server monitor
    Configuring SIP Server Monitor.
(config-sip-server-monitor)#recover responses 7 interval 32
```

The following example configures the SIP server monitor to send recover poll requests to the SIP server at **60** second intervals:

```
(config-T01)#sip-server monitor
    Configuring SIP Server Monitor.
(config-sip-server-monitor)#recover no-response interval 60
```

SIP TLS PROFILE COMMAND SET

Session Initiation Protocol (SIP) Transport Layer Security (TLS) is a cryptographic protocol, intended to replace Secure Socket Layer, that provides communication security over the internet. TLS is used to authenticate communication peers through the exchange of symmetric keys and authentication certificates. The protocol certifies the relation between a certificate and its owner as well as administers the validity of certificates used between communication peers. TLS operates on top of an underlying transport protocol, such as Transport Control Protocol (TCP), which carries the encrypted data. Privacy and security is provided by TLS between media endpoints, particularly in SIP signaling in Voice over IP (VoIP) networks. The certificate authority (CA) profile is responsible for certificate storage and management. Each TLS profile is associated with exactly one CA profile. TLS is configurable on a per-Session Initiation Protocol (SIP) trunk basis by applying a TLS profile. The profile is used by each SIP/TLS entity, and contains the configuration necessary to control TLS usage, such as identity validation, negotiable cipher suites, CA profiles, and server or mutual authentication settings.

Each entity that uses TLS uses a TLS profile. Many TLS profiles can exist and be referenced by many entities using TLS on the AOS device. The same TLS profile can be used by as many entities using TLS as required. The TLS profile essentially operates as a template for TLS operation and is applied on a per-trunk basis.

TLS profiles are created and configured using the **tls-profile** <*profile name*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#tls-profile TLSPROFILE1
(config-tls-profile-TLSPROFILE1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

allow-self-signed-cert on page 4881
authentication mutual on page 4882
ca-profile <profile name> on page 4883
secure-ciphersuite <name> on page 4884
tls-version on page 4886
validate identity on page 4887

allow-self-signed-cert

Use the **allow-self-signed-cert** command to allow a Transport Layer Security (TLS) communication peer to send a self-signed certificate as its sole identification. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

A trusted copy of the peer's certificate must be specified in the certificate authority (CA) profile associated with the TLS profile in order to validate the certificate provided by the peer in the TLS handshake. If this feature is not enabled, the peer's certificate must be signed by a trusted CA.

Usage Examples

The following example configures the TLS profile to allow a TLS peer to send a self-signed certificate as identification:

(config)**#tls-profile TLSPROFILE1**
(config-tls-profile-TLSPROFILE1)**#allow-self-signed-cert**

authentication mutual

Use the **authentication mutual** command to enable mutual Transport Layer Security (TLS) authentication in the TLS profile. Use the **no** form of this command to disable mutual authentication and return to the default authentication method (server authentication).

Syntax Description

No subcommands.

Default Values

By default, TLS mutual authentication is disabled and server authentication is used.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

If mutual authentication is configured, when the entity using the TLS profile is responding to a TLS negotiation (server role), the server requests the certificate of authentication from the client, and then authenticates the client. If the client does not provide a certificate, or the certificate fails validation, the TLS connection is rejected by the server. If mutual authentication is not configured, the responder (server) does not request or require a certificate from the client. When the entity using the TLS profile is initiating a Session Initiation Protocol (SIP)/TLS negotiation (client role), the client always requests the certificate of authentication and then authenticates the server. If the server does not provide a certificate or the certificate fails validation, the TLS connection is rejected by the client.

Usage Examples

The following example enables mutual authentication in the TLS profile:

(config)**#tls-profile TLSPROFILE1**
(config-tls-profile-TLSPROFILE1)**#authentication mutual**

ca-profile *<profile name>*

Use the **ca-profile** command to apply a previously configured certificate authority (CA) profile to the TLS profile. Use the **no** form of this command to remove the CA profile from the TLS profile.

Syntax Description

<profile name>	Specifies the name of the previously created CA profile.

Default Values

By default, no CA profile is associated with the TLS profile.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

A CA profile must be specified for TLS operation. The TLS profile is not valid until it is associated with a valid CA profile. If the command is entered more than once, the previous instance of the command is overwritten.

TLS authentication modes support both server authentication and mutual authentication. In most Session Initiation Protocol (SIP) applications, a SIP entity using TLS might initiate or respond to a TLS connection at any given time and therefore would be configured to operate as client or server. For example, trunks would typically operate as peers and use mutual authentication and SIP phones would typically be authenticated using server authentication. If the CA profile limits TLS authentication to a single mode of authentication (either server or mutual), the CA profile could omit the trusted or self-signed certificate. This is a rare case, however, since most SIP entities can be servers or clients at any time.

For more information about configuring CA profiles, refer to the *CA Profile Command Set on page 5209*.

Usage Examples

The following example associates the CA profile **MYPROFILE** with the TLS profile:

(config)**#tls-profile TLSPROFILE1**
(config-tls-profile-TLSPROFILE1)**#ca-profile MYPROFILE**

secure-ciphersuite <*name*>

Use the **secure-ciphersuite** command to specify a Transport Layer Security (TLS) cipher suite for the TLS profile. Use the **no** form of this command to remove the cipher suite from the TLS profile. Variations of this command include:

secure-ciphersuite <*name*>
secure-ciphersuite <*name*> <*number*>

Syntax Description

<*name*>	Specifies the name of a supported TLS cipher suite. Supported cipher suites are as follows: **TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA** **TLS_DHE_RSA_WITH_AES_128_CBC_SHA** **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384** **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256** **TLS_DHE_RSA_WITH_AES_256_CBC_SHA** **TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384** **TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384** **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** **TLS_RSA_WITH_3DES_EDE_CBC_SHA** **TLS_RSA_WITH_AES_128_CBC_SHA** **TLS_RSA_WITH_AES_256_CBC_SHA** **TLS_RSA_WITH_NULL_MD5** **TLS_RSA_WITH_NULL_SHA** **TLS_RSA_WITH_RC4_128_MD5** **TLS_RSA_WITH_RC4_128_SHA**
<*number*>	Optional. Specifies an integer that describes the cipher suite's desired relative position among all enabled cipher suites within the profile. Valid range is **1** to **65535**.

Default Values

By default, all strong (high level) cipher suites are individually enabled and all weak cipher suites are individually disabled.

Command History

Release R11.5.0	Command was introduced.
Release R13.1.0	Command was expanded to include the **TLS_DHE_RSA_WITH_AES_256_CBC_SHA256** and **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384** cipher suites.

Functional Notes

If multiple cipher suites have the same number value specified, they are placed in that number position and then subsorted in the order they appear in the configuration. One instance of this command exists for each supported TLS cipher suite.

Usage Examples

The following example enables a cipher suite in the TLS profile:

(config)**#tls-profile TLSPROFILE1**
(config-tls-profile-TLSPROFILE1)**#secure-ciphersuite TLS_RSA_WITH_RC4_128_SHA 150**

tls-version

Use the **tls-version** command to specify the Transport Layer Security (TLS) version used by this TLS profile. Use the **no** form of this command to revert to the default TLS version. Variations of this command include:

tls-version 1.0
tls-version 1.1
tls-version 1.2
tls-version fallback
tls-version fallback 1.0
tls-version fallback 1.1
tls-version fallback 1.2

Syntax Description

1.0	Specifies TLS version 1.0 is used.
1.1	Specifies TLS version 1.1 is used.
1.2	Specifies TLS version 1.2 is used.
fallback	Specifies that fallback from the highest supported TLS version to the lowest supported version is allowed.
fallback 1.0	Specifies that fallback from the highest supported TLS version to 1.0 is allowed.
fallback 1.1	Specifies that fallback from the highest supported TLS version to 1.1 is allowed.
fallback 1.2	Specifies that fallback from the highest supported TLS version to 1.2 is allowed.

Default Values

By default, fallback 1.2 is enabled.

Command History

Release R11.5.0	Command was introduced.
Release R13.8.0	Command was expanded to include the **fallback [1.0 | 1.1 | 1.2]** parameter.

Usage Examples

The following example specifies that the TLS profile uses TLS version **1.2**:

(config)**#tls-profile TLSPROFILE1**
(config-tls-profile-TLSPROFILE1)**#tls-version 1.2**

validate identity

Use the **validate identity** command to control how the identity of the Transport Layer Security (TLS) communication peer's certificate, received during the TLS handshake, is validated. Use the **no** form of this command to remove the identity validation method from the TLS profile. Variations of this command include:

validate identity fqdn configured
validate identity fqdn resolved
validate identity ip-address
validate identity string

Syntax Description

fqdn configured	Specifies that the peer's subject alternative name (SAN) IP domain naming service (DNS) name is used to validate the peer. The name must match the fully qualified domain name (FQDN) configured for the peer at the trunk.
fqdn resolved	Specifies that the peer's SAN IP domain DNS name is used to validate the peer. The name must match the FQDN as resolved by DNS service records (SRVs) from the FQDN as configured for the peer at the trunk.
ip-address	Specifies that the peer's SAN IP address is used to validate the peer. The address must match the IP address configured or resolved by DNS for the peer at the trunk.
string	Specifies that the peer's SAN fields or Subject components are used to identify the peer. The string must match the string configured at the trunk (using the command *peer-certificate-identity <string> on page 5108*).

Default Values

By default, identity validations are disabled and only proper signing is verified.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Up to one instance of each validation method can be specified in the profile, and each method specified must be matched in order for successful validation. These identity validation methods do not specify the value that must be matched, but rather specify an attribute whose value is related to the current session.

Usage Examples

The following example enables identity validation for the TLS profile based on IP address:

(config)**#tls-profile TLSPROFILE1**
(config-tls-profile-TLSPROFILE1)**#validate identity ip-address**

SRTP PROFILE COMMAND SET

Secure Realtime Transfer Protocol (SRTP) is a protocol used to provide confidentiality, message authentication, and replay protection to Realtime Transfer Protocol (RTP) traffic. This protocol provides a framework for encryption and message authentication of RTP streams between media endpoints. Typically, SRTP uses Transport Layer Security (TLS) for signaling authentication and encryption. Although SRTP protects the media shared between endpoints, it relies on the exchange of Session Description Protocol Security Descriptions (SDES) keys that appear clearly within the SIP message. TLS is used with SRTP to encrypt the signaling and protect against snooping of the SDES keys. TLS is not required for successful SRTP negotiation, but it is strongly recommended. In AOS, SRTP is used for calls when SRTP is enabled and when the capabilities of the communication peer allow it. SRTP configuration in AOS depends on the configuration of an SRTP profile. This profile controls SRTP usage for AOS devices acting as communication servers and is applied on a per-trunk basis in the AOS device.

Each entity that uses SRTP uses an SRTP profile. Many SRTP profiles can exist and be referenced by many entities using SRTP on the AOS device. The same SRTP profile can be used by as many entities using SRTP as required. The SRTP profile essentially operates as a template for SRTP operation and is applied on a per-trunk basis.

SRTP profiles are created and configured using the **srtp-profile** <*profile name*> command from the Global Configuration mode as follows:

```
>enable
#configure terminal
(config)#tls-profile SRTPPROFILE1
(config-srtp-profile-SRTPPROFILE1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

crypto-suite <crypto suite> on page 4889
srtcp on page 4890
srtp auth on page 4891
srtp encrypt on page 4892

crypto-suite *<crypto suite>*

Use the **crypto-suite** command to specify a Secure Realtime Transfer Protocol (SRTP) cryptography suite for the SRTP profile. Use the **no** form of this command to remove the crypto suite from the SRTP profile.

Syntax Description

<crypto suite> Specifies the SRTP crypto suite to use in this profile. Supported SRTP crypto suites are as follows:

SRTP Crypto Suites	Associated RFC
AES_CM_128_HMAC_SHA1_80	RFC 4568
AES_CM_128_HMAC_SHA1_32	RFC 4568
AES_256_CM_HMAC_SHA1_80	RFC 6188
AES_256_CM_HMAC_SHA1_32	RFC 6188
SRTP_NULL_HMAC_SHA1_80	RFC 3711
SRTP_NULL_HMAC_SHA1_32	RFC 3711

Default Values

By default, the **AES_CM_128_HMAC_SHA1_80** crypto suite is used.

Command History

Release R11.5.0 Command was introduced.

Usage Examples

The following example specifies the SRTP crypto suite to be used with this profile:

(config)**#srtp-profile SRTPPROFILE1**
(config-srtp-profile-SRTPPROFILE1)**#crypto-suite SRTP_NULL_HMAC_SHA1_80**

srtcp

Use the **srtcp** command to specify the Secure Realtime Transport Control Protocol (SRTCP) encryption method for the Secure Realtime Transport Protocol (SRTP) profile. Variations of this command include:

srtcp encrypt
srtcp offer-no-encrypt
srtcp strict-no-encrypt

Syntax Description

encrypt	Species that the SRTP session must encrypt SRTP.
offer-no-encrypt	Specifies that encryption can be used, but is not required.
strict-no-encrypt	Specifies that session must not encrypt SRTCP.

Default Values

By default, the SRTP session must encrypt SRTCP.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

When **encrypt** is used, as an offerer, the crypto attributes offered do not contain the UNENCRYPTED_SRTCP parameter and answers that contain this parameter are not accepted.

When **offer-no-encrypt** is used, as an offerer, the crypto attributes offered contain the UNENCRYPTED_SRTCP session parameter, and valid answers with or without the parameter are accepted. When enabled as an answerer, a crypto attribute with or without the UNENCRYPTED_SRTCP parameter can be selected.

When **strict-no-encrypt** is used, as an offerer, the crypto attributes offered contain the UNENCRYPTED_SRTCP session parameter and answers not containing the same parameter are not accepted. When enabled as an answerer, the crypto attribute that does not contain the UNENCRYPTED_SRTCP parameter is rejected.

The SRTP authentication and encryption commands (*srtp auth on page 4891* and *srtp encrypt on page 4892*), as well as this SRTCP encryption command, are set once at the SRTP profile but they affect the parameter present in each crypto attribute associated with a media session.

Usage Examples

The following example specifies that the SRTP profile does not encrypt SRTCP:

(config)**#srtp-profile SRTPPROFILE1**
(config-srtp-profile-SRTPPROFILE1)**#srtcp strict-no-encrypt**

srtp auth

Use the **srtp auth** command to specify the Secure Realtime Transfer Protocol (SRTP) authentication method for the SRTP profile. Variations of this command include:

srtp auth
srtp offer-no-auth
srtp strict-no-auth

Syntax Description

auth	Specifies that the SRTP session must authenticate SRTP.
offer-no-auth	Specifies that the SRTP session can authenticate SRTP, but it is not required.
strict-no-auth	Specifies that the SRTP session must not authenticate SRTP.

Default Values

By default, SRTP sessions must authenticate SRTP.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

When **auth** is used, as an offerer, the crypto attributes offered do not contain the UNAUTHENTICATED_SRTP session parameter, and any answers containing that parameter are not accepted. When enabled as an answerer, the crypto attribute containing the same parameter is not accepted.

When **offer-no-auth** is used, as an offerer, crypto attributes offered contain the UNAUTHENTICATED_SRTP parameter, and valid answers with or without that parameter are accepted. When enabled as an answerer, the crypto attribute with or without this parameter can be selected.

When **strict-no-auth** is used, as an offerer, crypto attributes offered contain the session parameter UNAUTHENTICATED_SRTP and answers that do NOT contain this parameter are rejected. When enabled as an answerer, the crypto attribute containing the parameter is not accepted.

The SRTP authentication and encryption commands (*srtp auth on page 4891* and *srtp encrypt on page 4892*), as well as the SRTCP encryption command (*srtcp on page 4890*), are set once at the SRTP profile but they affect the parameter present in each crypto attribute associated with a media session.

Usage Examples

The following example specifies that the SRTP profile authenticates with or without the UNAUTHENTICATED_SRTP parameter:

(config)**#srtp-profile SRTPPROFILE1**
(config-srtp-profile-SRTPPROFILE1)**#srtp offer-no-auth**

srtp encrypt

Use the **srtp encrypt** command to specify the Secure Realtime Transfer Protocol (SRTP) encryption method for the SRTP profile. Variations of this command include:

srtp encrypt
srtp offer-no-encrypt
srtp strict-no-encrypt

Syntax Description

encrypt	Specifies that the SRTP session must encrypt SRTP.
offer-no-encrypt	Specifies that the SRTP session can encrypt SRTP, but it is not required.
strict-no-encrypt	Specifies that the SRTP session must not encrypt SRTP.

Default Values

By default, SRTP sessions must encrypt SRTP.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

When **encrypt** is used, as an offerer, the crypto attributes offered do not contain the UNENCRYPTED_SRTP session parameter, and any answers containing that parameter are not accepted.

When **offer-no-encrypt** is used, as an offerer, crypto attributes offered contain the UNUNENCRYPTED_SRTP parameter, and valid answers with or without that parameter are accepted. When enabled as an answerer, the crypto attribute with or without this parameter can be selected.

When **strict-no-encrypt** is used, as an offerer, crypto attributes offered contain the session parameter UNENCRYPTED_SRTP and answers that do NOT contain this parameter are rejected. When enabled as an answerer, the crypto attribute containing the parameter is not accepted.

The SRTP authentication and encryption commands (*srtp auth on page 4891* and *srtp encrypt on page 4892*), as well as the SRTCP encryption command (*srtcp on page 4890*), are set once at the SRTP profile but they affect the parameter present in each crypto attribute associated with a media session.

Usage Examples

The following example specifies that the SRTP profile is accepted with or without encryption:

(config)**#srtp-profile SRTPPROFILE1**
(config-srtp-profile-SRTPPROFILE1)**#srtp offer-no-encrypt**

VOICE CODEC LIST COMMAND SET

Voice coder-decoder (CODEC) lists are lists of CODECs arranged in preferred order with the first listed CODEC being the most preferred for call negotiation.

The primary reason to create and assign voice CODEC lists is to save time. CODEC lists are created, listing CODECs in the order of preference, and then lists are applied to interfaces using the **codec-group** command (refer to the specific interface configuration command set for more information). Configuring a CODEC list allows the list to be applied to multiple interfaces, such as Media Gateway Control Protocol (MGCP) interfaces, voice trunks, voice accounts, and voice users without having to define the order of CODECs individually. The order of preference is used primarily to conserve bandwidth on wide area network (WAN)-based interfaces.

For example, when a user makes an outbound call from a foreign exchange station (FXS) port to a Session Initiation Protocol (SIP) trunk, the trunk will look at its CODEC list and query the user making the call as to which CODEC is to be used according to its CODEC list. It will query with the first CODEC (for example, G.729). If this CODEC is listed in the CODEC list that is applied to the user (no matter the CODEC preference on the user interface), then G.729 is agreed upon and the call will be converted and sent out the trunk. This is the most bandwidth conservative CODEC in this case.

To activate the Voice CODEC List Configuration mode, enter the **voice codec-list trunk** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice codec-list List1
(config-codec)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

codec on page 4894
default on page 4896

codec

Use the **codec** command to specify the order of preference for coder-decoders (CODECs) used by the CODEC list. Use the **no** form of this command to remove a CODEC from the CODEC list. Variations of this command include:

codec g711alaw
codec g711ulaw
codec g722
codec g729

Syntax Description

g711alaw	Assigns the G.711 A-law CODEC (64000 bps) as the preferred CODEC for negotiation.
g711ulaw	Assigns the G.711 U-law CODEC (64000 bps) as the preferred CODEC for negotiation.
g722	Assigns the G.722 CODEC as the preferred CODEC for negotiation.
g729	Assigns the G.729 CODEC (8000 bps) as the preferred CODEC for negotiation.

Default Values

By default, no CODEC lists are created.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was expanded to include the **g711alaw** parameter.
Release A2.04	Command was expanded to include the **g722** parameter.

Functional Notes

You can enter as many CODECs in the list as necessary by repeating the **codec** command while in the Voice CODEC List Configuration mode (refer to the *Usage Examples* section of this command).

Order is important when creating a CODEC list. The interface attempts to use the first CODEC in the list to negotiate a call. If the first CODEC negotiation is unsuccessful, the interface uses the second CODEC in the list and so on. If this process is unsuccessful, the call will fail.

CODEC lists do not take any action until they are applied to an interface. For information on applying CODEC lists, refer to the **codec-group** <*name*> command in the command section of the interface to which you want to apply the list.

Usage Examples

The following example creates a CODEC list, **List1**, and specifies that the interface to which this list is applied will use **g729** first, **g711ulaw** second, and **g722** third as it negotiates the call:

(config)**#voice codec-list List1**
(config-codec)**#codec g729**
(config-codec)**#codec g711ulaw**
(config-codec)**#codec g722**

default

Use the **default** command to set the coder-decoder (CODEC) list as the default list for call negotiation on the interface to which it is applied. Use the **no** form of this command to remove the CODEC list as the default.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example specifies the CODEC list **List1** is used as the default list for call negotiation on the interfaces to which the list is applied:

(config)**#voice codec-list List1**
(config-codec)**#default**

VOICE COS COMMAND SET

Class of service (CoS) defines the permissions available to a system user for making voice calls, and it is necessary to configure CoS before calls can be made (other than to the operator and 911). Voice CoS permissions include the types of calls and actions a user can perform. There are three default classes of voice CoS: normal users, executive users, and public phones, but you can also create your own class. A maximum of 10 voice CoS types can be defined. The commands in this section help you to define voice CoS classes so they can be applied to voice users. Voice CoS classes created with these commands are applied to users using the **cos** command, detailed in the *Voice User Account Command Set on page 4564*. For more information on configuring voice CoS, refer to the *NetVanta 7000 Series Classes of Service* quick configuration guide available online at https://supportcommunity.adtran.com.

To create a voice CoS and enter the Voice CoS Configuration mode, enter the **voice class-of-service** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

aa-initiate-permit <template> on page 4899
block-caller-id on page 4901
call-privilege on page 4902
camp-on on page 4904
conference on page 4905
default-level on page 4906
deny-template <template> on page 4907
disable-callwaiting on page 4909
dnd on page 4910
door-phone on page 4911
external-fwd on page 4912
forward on page 4913
hold on page 4914

aa-initiate-permit *<template>*

Use the **aa-initiate-permit** command to enable the handsfree auto answer feature. Handsfree voice communication (similar to using a speakerphone or intercom) will be available for the programmed number template. When using **aa-initiate-permit**, the receiving party's phone automatically answers the phone. Use the **no** form of this command to disable this feature.

Syntax Description

<template>	Allows users with the specified number template to initiate auto answer calls. Refer to *Functional Notes* for more information.

Default Values

By default, **aa-initiate-permit** is disabled.

Command History

Release 13.1	Command was introduced.

Functional Notes

In order to place an auto answer call, you must dial ** prior to the number. Users can also program ** as a soft key to dial ** separately before dialing the number to call. Users must dial ***971** to block auto answer calls and ***970** to reactivate the feature.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example enables the handsfree auto answer for users with the extension range of **4200** to **4299**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#aa-initiate-permit 42xx**

block-caller-id

Use the **block-caller-id** command to conceal caller ID information for outbound calls. Use the **no** form of this command to allow caller ID for outbound calls.

Syntax Description

No subcommands.

Default Values

By default, the **block-caller-id** feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example blocks caller ID for outbound calls in rule set **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#block-caller-id
```

call-privilege

Use the **call-privilege** command to assign general call privileges for outbound access. This determines what type of calls a user is permitted to make as a member of this class of service (CoS). Use the **no** form of this command to remove general call privileges for outbound access. Variations of this command include:

call-privilege 900-number
call-privilege all
call-privilege extensions
call-privilege international
call-privilege local
call-privilege long-distance
call-privilege operator-assisted
call-privilege specify-carrier
call-privilege toll-free
call-privilege [user1 | user2 | user3]

Syntax Description

900-number	Permits 900 calls in the form 1-900-NXX-XXXX and 976-XXXX.
all	Permits all calls.
extensions	Permits internal calls.
international	Permits international calls in the form 011-number.
local	Permits local calls in the form NXX-XXXX.
long-distance	Permits long distance calls in the form 1-NXX-NXX-XXXX.
operator-assisted	Permits operator-assisted calls.
specify-carrier	Permits calls that specify carrier.
toll-free	Permits toll free calls.
user1	Permits calls that match the first user-defined template.
user2	Permits calls that match the second user-defined template.
user3	Permits calls that match the third user-defined template.
	Valid characters include: 0-9 - Any single digit. X - Any single digit 0 through 9. N - Any single digit 2 through 9.

Default Values

By default, no call privileges are enabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example permits long distance calls in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#call-privilege long-distance**

camp-on

Use the **camp-on** command to allow automatic retry of a busy extension. This feature enables a user to reach the busy party as soon as the line is available. Use the **no** form of this command to disable automatic retry.

Syntax Description

No subcommands.

Default Values

By default, the **camp-on** feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables automatic retry of a busy extension in rule set **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#camp-on
```

conference

Use the **conference** command to allow the initiation of three-way conference calls. This feature allows multiple parties to communicate at the same time on the same line. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the three-way conference call feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example allows the initiation of three-way conference calls in rule set **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#conference
```

default-level

Use the **default-level** command to set this class of service (CoS) level as the default. When enabled, new users that are added to the system are assigned this CoS by default. To change the default from this CoS level, use the **no** form of this command.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the rule set **set1** as the default CoS level:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#default-level**

deny-template *<template>*

Use the **deny-template** command to configure a number template that specifies the types of calls that users in this class of service (CoS) are not allowed to make. Use the **no** form of this command to remove a deny template.

Syntax Description

<template>	Specifies a number template. All calls matching this pattern will be denied. Refer to *Functional Notes* for more information.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Functional Notes

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example denies users in rule set **set1** the ability to make any call beginning with **555**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#deny-template 555-xxxx**

disable-callwaiting

Use the **disable-callwaiting** command to allow users to control the call waiting feature. Disabling call waiting will block the alert of an incoming call while the user is on the phone. Use the **no** form of this command to enable call waiting.

Syntax Description

No subcommands.

Default Values

By default, call waiting is enabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to disable call waiting:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#disable-callwaiting**

dnd

Use the **dnd** command to enable do-not-disturb (DND). Do-not-disturb makes the line appear busy to incoming calls. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, the do-not-disturb feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables the do-not-disturb feature in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#dnd**

door-phone

Use the **door-phone** command to allow the user to call the door phone using a special prefix (SPRE) code. Use the **no** form of this command to deny door phone access.

Syntax Description

No subcommands.

Default Values

By default, door phone access is denied.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example allows door phone access in voice class of service (CoS) rule set named **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#door-phone**

external-fwd

Use the **external-fwd** command to allow forwarding of calls to an external number. When enabled, the users can forward their phones to lines outside the system, such as their home numbers. Use the **no** form of this command to disable external call forwarding.

Syntax Description

No subcommands.

Default Values

By default, forwarding calls to an external number is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to forward calls to an external number:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#external-fwd
```

forward

Use the **forward** command to allow users to forward calls to another extension. Forwarding calls allows the user to receive incoming calls at a different number. Use the **no** form of this command to end call forwarding.

Syntax Description

No subcommands.

Default Values

By default, internal call forwarding is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to forward calls:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#forward**

hold

Use the **hold** command to allow users to place calls on standby. Use the **no** form of this command to disable the call hold option.

Syntax Description

No subcommands.

Default Values

By default, the call hold option is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables users in rule set **set1** to place a call on hold:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#hold**

hotel

Use the **hotel** command to allow extension reassignment to an alternate phone. Use the **no** form of this command to disable extension reassignment.

Syntax Description

No subcommands.

Default Values

By default, the **hotel** feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables users in rule set **set1** to reassign an extension to an alternate phone:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#hotel
```

logout-group

Use the **logout-group** command to allow a user to issue a special prefix (SPRE) command to log out of a user group. Use the **no** form of this command to deny the ability to log out of a user group.

Syntax Description

No subcommands.

Default Values

By default, the ability to log out of a user group is denied.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example allows the user in rule set **set1** to log out of a user group:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#logout-group
```

message-waiting

Use the **message-waiting** command to allow message waiting indicator control. This allows users to change the manner in which message notification takes place. Use the **no** form of this command to disable message waiting indicator control.

Syntax Description

No subcommands.

Default Values

By default, control of the message waiting indicator is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to manage message waiting indicators:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#message-waiting**

overhead-paging

Use the **overhead-paging** command to allow the user to connect to overhead paging using a special prefix (SPRE) code. Use the **no** form of this command to deny the ability to connect to overhead paging.

Syntax Description

No subcommands.

Default Values

By default, the ability to connect to overhead paging is denied.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example allows the user in rule set **set1** to connect to overhead paging:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#overhead-paging**

override-passcode <*passcode*>

Use the **override-passcode** command to assign an override passcode. This four-digit code is used in conjunction with the class of service (CoS) override feature and enables a user to override an extension's configured CoS with the new CoS as defined by the passcode. Use the **no** form of this command to remove an override passcode.

Syntax Description

<*passcode*>	Specifies a four-digit numerical passcode.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the override passcode to **1234** in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level "set1".
(config-cos-set1)**#override-passcode 1234**

park

Use the **park** command to allow users to park calls on the system. Use the **no** form of this command to disable the call parking feature.

Syntax Description

No subcommands.

Default Values

By default, the parking feature is enabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example allows users to park calls in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#park**

permit template <*number*>

Use the **permit template** command to configure call privilege additions that are permitted access only. This specifically allows an otherwise restricted number to be dialed. Use the **no** form of this command to remove the template.

Syntax Description

<*number*>	Specifies the number that may be dialed. The number is in the form **NXX-XXXX**, where **N** is **2** to **9** and **X** is **0** to **9**.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example allows the number **325-1234** to be dialed in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#permit template 325-1234**

pickup

Use the **pickup** command to enable the call pickup feature. If enabled, users with this voice class of service (CoS) applied can enter a special prefix (SPRE) code or group extension to answer calls ringing on another phone. Using the **no** form of this command disabled the call pickup feature on the CoS.

Syntax Description

No subcommands.

Default Values

By default, call pickup is disabled.

Command History

Release A4.01	Command was introduced.

Functional Notes

There are two types of call pickup available: directed call pickup and call pickup groups. Directed call pickup allows a user to answer a ringing phone by dialing a SPRE code in addition to the phone's extension. For example, using directed call pickup, a user would dial ***528509** where ***52** is the call pickup SPRE code and **8509** is the ringing phone's extension. Call pickup groups allow the user to dial the group extension to answer the ringing phone. For more information about configuring call pickup, refer to the *Configuring the Call Pickup Feature on AOS Voice Products* quick configuration guide available online at https://supportcommunity.adtran.com.

Usage Examples

The following example enables the call pickup feature in the CoS **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level "set1".
(config-cos-set1)#pickup
```

program-user-speed

Use the **program-user-speed** command to allow users to access speed dial functionality through the system. Use the **no** form of this command to disable the speed dialing feature.

Syntax Description

No subcommands.

Default Values

By default, the speed dial feature is disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables the speed dial feature for users in rule set **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#program-user-speed
```

redial

Use the **redial** command to grant users access to the redial functionality, which redials the last outgoing number. Use the **no** form of this command to disable last number redial.

Syntax Description

No subcommands.

Default Values

By default, the last number **redial** feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables the last number redial feature in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#redial**

remote-fwd

Use the **remote-fwd** command to allow a user to control call forwarding from a remote location. Use the **no** form of this command to disable remote forwarding.

Syntax Description

No subcommands.

Default Values

By default, remote forwarding feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to enable call forwarding from a remote location:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#remote-fwd
```

rename *<name>*

Use the **rename** command to assign a new name to the class of service (CoS) rule set.

Syntax Description

<name>	Specifies the new name of the CoS rule set.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example changed the name of rule set **set1** to **accounting**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#rename accounting**
(config-cos-accounting)#

retrieve-park

Use the **retrieve-park** command to allow the retrieval of parked calls. Use the **no** form of this command to disable the retrieve parked calls feature.

Syntax Description

No subcommands.

Default Values

By default, the retrieve parked calls feature is disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables retrieval of parked calls in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#retrieve-park**

return-last-call

Use the **return-last-call** command to allow users to return the last call received. Use the **no** form of this command to disable the return last call received feature.

Syntax Description

No subcommands.

Default Values

By default, the **return-last-call** feature is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to return the last call received:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#return-last-call**

send-to-vm

Use the **send-to-vm** command to allow users to send calls directly to voicemail. Use the **no** form of this command to disable the ability to send calls to directly to voicemail.

Syntax Description

No subcommands.

Default Values

By default, the ability to send calls directly to voicemail is disabled.

Command History

Release R10.2.0	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to send calls directly to voicemail:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#send-to-vm
```

station-lock

Use the **station-lock** command to allow users to lock an extension, preventing it from making outbound calls. Use the **no** form of this command to revoke user's ability to disable outbound calling capabilities.

Syntax Description

No subcommands.

Default Values

By default, the **station-lock** feature is disabled. Users are not allowed to block their extension's capability to place outbound calls.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables the station-lock feature in rule set **set1**:

(config)**#voice class-of-service set1**
Configuring Existing Level "set1".
(config-cos-set1)**#station-lock**

system-mode

Use the **system-mode** command to enable the system mode feature for this class of service (CoS). Once enabled, users to whom this CoS is applied can activate different system modes on the unit via the command line interface (CLI), special prefix (SPRE) codes, auto attendant, or the Web-based graphical user interface (GUI). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release A1	Command was introduced.

Usage Examples

The following example enables the system mode feature for users with the applied CoS **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#system-mode
```

system-speed

Use the **system-speed** command to enable system speed dial usage for the system. Use the **no** form of this command to disable the system speed setting.

Syntax Description

No subcommands.

Default Values

By default, **system-speed** is enabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables configuration of the system speed in rule set **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#system-speed
```

transfer

Use the **transfer** command to allow users to perform call transfers. Use the **no** form of this command to disable call transfers.

Syntax Description

No subcommands.

Default Values

By default, the call transfer feature is disabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to perform call transfers:

(config)**#voice class-of-service set1**
Configuring Existing Level “set1”.
(config-cos-set1)**#transfer**

unlock-door

Use the **unlock-door** command to enable the user to use a special prefix (SPRE) code to control the door contact. Use the **no** form of this command to disable door contact operation.

Syntax Description

No subcommands.

Default Values

By default, door contact operation is disabled.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example enables door contact operation in rule set **set1**:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#unlock-door
```

user-speed

Use the **user-speed** command to allow users to program speed dial numbers. Use the **no** form of this command to deny this privilege.

Syntax Description

No subcommands.

Default Values

By default, user speed dial programming is not allowed.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example allows users in rule set **set1** to program speed dial numbers:

```
(config)#voice class-of-service set1
Configuring Existing Level “set1”.
(config-cos-set1)#user-speed
```

VOICEMAIL COS COMMAND SET

Class of service (CoS) defines the permissions available to a system user, and in this case defines permissions as they relate to user voicemail. By default, users are not assigned a voicemail CoS. When a user's account does not have an assigned voicemail CoS, the user will not have access to a voice mailbox. The commands in this section help you to create a CoS specifically for voice mailboxes. The classes created with these commands are then applied to users using the command *voicemail on page 4646*. For more information about configuring voicemail CoS and voicemail in general, refer to the *NetVanta 7000 Series Voicemail* quick configuration guide available online at https://supportcommunity.adtran.com.

To create a voicemail CoS and enter the Voicemail CoS Configuration mode, enter the **voice mail class-of-service** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice mail class-of-service class1
Configuring Existing Level "class1".
(config-vm-class1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

default-level on page 4937
expire-time <days> on page 4938
greeting-length-max <time> on page 4939
greeting-quota <time> on page 4940
message-length-max <time> on page 4941
message-quota <time> on page 4942
prompt-delete on page 4943
rename <name> on page 4944

default-level

Use the **default-level** command to set the current voicemail class of service (CoS) level as the default level. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example configures the voicemail CoS **class1** as the default CoS:

(config)**#voice mail class-of-service class1**
Configuring Existing Level "class1".
(config-vm-class1)**#default-level**

expire-time *<days>*

Use the **expire-time** command to set the number of days before a voicemail message expires. Use the **no** form of this command to return to the default value.

Syntax Description

<days>	Specifies the number of days until a message expires. Valid range is **5** to **60** days. A value of **0** means messages will never expire.

Default Values

By default, the number of days is set to **0**, which means messages will never expire.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the voicemail class of service (CoS) **class1** to delete voicemail messages after **14** days:

(config)**#voice mail class-of-service class1**
Configuring Existing Level "class1".
(config-vm-class1)**#expire-time 14**

greeting-length-max *<time>*

Use the **greeting-length-max** command to set the maximum length (in seconds) for a voicemail greeting. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the length in seconds for a voicemail greeting. Valid range is **20** to **120** seconds.

Default Values

By default, the maximum voicemail greeting time is set to **60** seconds.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the maximum length for a voicemail greeting in rule set **class1** to **60** seconds:

(config)**#voice mail class-of-service class1**
Configuring Existing Level "class1".
(config-vm-class1)**#greeting-length-max 60**

greeting-quota *<time>*

Use the **greeting-quota** command to set the maximum storage time (in minutes) of all greeting messages. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the maximum storage time (in minutes) for the storage of all greeting messages. Valid range is **1** to **9** minutes.

Default Values

By default, the maximum storage time for all greeting messages is **3** minutes.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the maximum storage time for all greeting messages in rule set **class1** to **5** minutes:

(config)**#voice mail class-of-service class1**
Configuring Existing Level "class1".
(config-vm-class1)**#greeting-quota 5**

message-length-max *<time>*

Use the **message-length-max** command to set the maximum length (in seconds) for a voicemail message. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the maximum length (in seconds) for a voicemail message. Valid range is **30** to **600** seconds.

Default Values

By default, the maximum length for a voicemail message is **120** seconds.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example sets the maximum length a voicemail message in rule set **class1** to **300** seconds:

(config)**#voice mail class-of-service class1**
Configuring Existing Level "class1".
(config-vm-class1)**#message-length-max 300**

message-quota *<time>*

Use the **message-quota** command to set the maximum storage time (in minutes) of all voicemail messages. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the maximum storage time (in minutes) of all voicemail messages. Valid range is **1** to **180** minutes.

Default Values

By default, the maximum storage time of all voicemail messages is **10** minutes.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example sets the maximum storage time of all voicemail messages in rule set **class1** to **120** minutes:

(config)**#voice mail class-of-service class1**
Configuring Existing Level "class1".
(config-vm-class1)**#message-quota 120**

prompt-delete

Use the **prompt-delete** command to configure the unit to prompt the user before deleting messages. Use the **no** form of this command to disable the prompt before deleting messages.

Syntax Description

No subcommands.

Default Values

By default, the prompt before deleting messages is disabled.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the unit to prompt the user before deleting voicemail messages:

```
(config)#voice mail class-of-service class1
Configuring Existing Level "class1".
(config-vm-class1)#prompt-delete
```

rename *<name>*

Use the **rename** command to rename the voicemail class of service (CoS) rule set. Use the **no** form of this command to return to the previous name.

Syntax Description

<name>	Specifies the new name of the CoS rule set.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example assigns a new name (**class2**) to the current CoS rule set **class1**:

(config)**#voice mail class-of-service class1**
Configuring Existing Level "class1".
(config-vm-class1)**#rename class2**

VQM REPORTER COMMAND SET

Voice quality monitoring (VQM) allows real time passive Voice over IP (VoIP) quality measurements to be taken on all Realtime Transport Protocol (RTP) voice streams transmitted through an AOS device. The VQM reporter is a feature supported by AOS devices that allows the gathered VQM statistics to be aggregated by third-party collectors, such as the n-Command® managed service provider (MSP) server. Allowing aggregation by the n-Command MSP server provides more flexibility in monitoring voice networks.

VQM should be enabled and configured on the AOS device before configuring the VQM reporter. For information on configuring VQM, refer to the *Voice Quality Monitoring* configuration guide available online at https://supportcommunity.adtran.com. VQM commands are also detailed in the *Global Configuration Mode Command Set on page 1149* beginning with the command *ip rtp quality-monitoring on page 1465*.

To create a VQM reporter and enter the reporter's configuration mode, enter the **ip rtp quality-monitoring reporter** <*name*> command from the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip rtp quality-monitoring reporter Reporter1
(config-rtp-reporter-Reporter1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
shutdown on page 93

All other commands in this command set are described in this section in alphabetical order:

collector on page 4946
collector auto-link on page 4948
domain <name> on page 4949
grammar contact host port persistent on page 4950
grammar from on page 4951
grammar request-uri on page 4952
grammar to on page 4953
max-queue-depth <value> on page 4954
max-retries <value> on page 4955
outbound-proxy on page 4956

collector

Use the **collector** command to specify the IP address or host name of the server that will be receiving information from the voice quality monitoring (VQM) reporter. Use the **no** form of this command to remove the server from the reporter's configuration. Variations of this command include:

collector primary <*hostname* | *ip address*>
collector primary <*hostname* | *ip address*> **tcp**
collector primary <*hostname* | *ip address*> **tcp** <*port*>
collector primary <*hostname* | *ip address*> **udp**
collector primary <*hostname* | *ip address*> **udp** <*port*>
collector primary <*hostname* | *ip address*> **tls** <*profile name*>
collector primary <*hostname* | *ip address*> **tls** <*profile name*> **srv**
collector primary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*>
collector primary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
collector primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*>
collector primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv**
collector primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
collector primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*> <*transport name prefix*>
collector secondary <*hostname* | *ip address*>
collector secondary <*hostname* | *ip address*> **tcp**
collector secondary <*hostname* | *ip address*> **tcp** <*port*>
collector secondary <*hostname* | *ip address*> **udp**
collector secondary <*hostname* | *ip address*> **udp** <*port*>
collector secondary <*hostname* | *ip address*> **tls** <*profile name*>
collector secondary <*hostname* | *ip address*> **tls** <*profile name*> **srv**
collector secondary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*>
collector secondary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
collector secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*>
collector secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv**
collector secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
collector secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*> <*transport name prefix*>

Syntax Description

primary	Specifies that the server is the primary contact server for the VQM reporter.
secondary	Specifies that the server is the secondary contact server for the VQM reporter.
<*hostname* | *ip address*>	Specifies the host name or IP address of the server. IP addresses should be expressed in the decimal dotted notation (for example, **10.10.10.1**).
tcp	Optional. Specifies that the reporter and server communicate using Transmission Control Protocol (TCP).

udp	Optional. Specifies that the reporter and server communicate using User Datagram Protocol (UDP).
tls *<profile name>*	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<port>	Optional. Specifies the port number used for communication between the reporter and the server. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<service name prefix>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<transport name prefix>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, no server is configured. When configured, by default, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release 17.6	Command was introduced.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Usage Examples

The following example specifies that the VQM reporter uses the server with the IP address of **172.5.67.99** as its **primary** server:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#collector primary 172.5.67.99**

The following example specifies the VQM collector as a primary collection server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#ip rtp quality-monitoring reporter REPORTER1**
(config-rtp-reporter-REPORTER1)**#collector primary 10.10.10.1 tls TLSPROFILE1**

collector auto-link

Use the **collector auto-link** command to specify the auto-link server that will be receiving information from the voice quality monitoring (VQM) reporter. When a failover event occurs, VQM reporters that are configured to use auto-link automatically roll over to the new server for reporting. Use the **no** form of this command to remove the auto-link server from the reporter's configuration. Variations of this command include:

collector auto-link
collector auto-link tcp
collector auto-link tcp *<port>*
collector auto-link udp
collector auto-link udp *<port>*

Syntax Description

tcp	Optional. Specifies that the reporter and server communicate using Transmission Control Protocol (TCP).
udp	Optional. Specifies that the reporter and server communicate using User Datagram Protocol (UDP).
<port>	Optional. Specifies the TCP or UDP port used for communication between the reporter and the server. Range is **0** to **65535**.

Default Values

By default, VQM reporting is not associated with an auto-link server.

Command History

Release R10.7.0	Command was introduced.

Usage Examples

The following example specifies that the VQM reporter uses the auto-link server and UDP:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#collector auto-link udp**

domain *<name>*

Use the **domain** command to configure the assigned fully qualified domain name (FQDN) for host messages. The domain is a unique identifier for the Session Initiation Protocol (SIP) messages sent by the VQM reporter. Use the no form of this command to disable this feature.

Syntax Description

<name>	Specifies the FQDN for the SIP messages sent by the VQM reporter.

Default Values

By default, no FQDN is configured.

Command History

Release R10.1.0	Command was introduced.

Usage Examples

The following example sets the domain name as **home.com**:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#domain home.com**

grammar contact host port persistent

Use the **grammar contact host port persistent** command to configure the AOS device to use the Transmission Control Protocol (TCP) port from which AOS initiated a Transport Layer Security (TLS) connection in the Contact uniform resource identifier (URI) sent by AOS. Use the **no** form of this command to disable this feature.

Syntax Description

host	Specifies the Contact header Host field setting.
port	Specifies the Contact header host port.
persistent	Specifies that the persistent connection port should be used for the Contact header host port.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced

Functional Notes

This configuration is useful when using client-only authentication. With this type of authentication, a persistent connection is established to the SIP server. Many SIP servers and enterprise session border controllers (eSBCs) need to see the TCP port from which AOS initiated the TLS connection in the Contact URI sent by AOS.

Usage Examples

The following example specifies that AOS device should use the TCP port from which AOS initiated the TLS connection in the Contact URI sent by AOS:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#grammar contact host port persistent**

grammar from

Use the **grammar from** command to configure the From header on Session Initiation Protocol (SIP) messages from the VQM reporter. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar from host collector
grammar from host domain
grammar from host local
grammar from user *<username>*
grammar from user none

Syntax Description

host	Specifies the Host field formatting for the From header.
collector	Specifies the collector's host setting for formatting the Host field of the From header.
domain	Specifies the user defined domain name for formatting the Host field of the From header. The domain name is configure using the command *domain <name> on page 4949*.
local	Specifies the local IP address for formatting the Host field of the From header.
user	Specifies the User field formatting for the From header.
<username>	Specifies the user name used to format the User field of the From header.
none	Specifies that the user is not include in the User field of the From header.

Default Values

By default, the host for formatting messages is **local**, and *<username>* is set to the unit's **serial number.**

Command History

Release A2	Command was introduced.
Release R10.1.0	Command was added to the VQM Reporter command set.

Usage Examples

The following example sets the From header format to use the user defined domain name:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#grammar from host domain**

The following example specifies that the user is not included in the User field of the From header:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#grammar from user none**

grammar request-uri

Use the **grammar request-uri** command to format the Request uniform resource identifier (URI) for Session Initiation Protocol (SIP) messages from the VQM reporter. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar request-uri host collector
grammar request-uri host domain
grammar request-uri host-resolve
grammar request-uri user follow-to
grammar request-uri user none

Syntax Description

host	Specifies the Host field formatting for the Request-URI header.
collector	Specifies the collector's host setting for formatting the Host field of the Request-URI header.
domain	Specifies the user defined domain name for formatting the Host field of the Request-URI header. The domain name is configure using the command *domain <name> on page 4949*.
host-resolve	Enables the local unit to resolve the domain before resolving the Host field of the Request URI.
user	Specifies the User field formatting for the Request-URI header.
follow-to	Specifies that the current To header user values should be used for formatting the User field formatting of the Request-URI header.
none	Specifies that the user is not included in the Request-URI header.

Default Values

By default, the host for formatting messages is **collector**, **host-resolve** is disabled, and the User field formatting uses the current To header (**follow-to**) user values.

Command History

Release A2	Command was introduced.
Release R10.1.0	Command was added to the VQM Reporter command set.

Usage Examples

The following example enables VQM reporter SIP messages to resolve the Request URI from the host domain:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#grammar request-uri host domain**

The following example specifies that the user is not included in the User field of the Request URI header:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#grammar request-uri user none**

grammar to

Use the **grammar to** command to configure the To header on Session Initiation Protocol (SIP) messages from the VQM reporter. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar to host collector
grammar to host domain
grammar to user <*username*>
grammar to user none

Syntax Description

host	Specifies the Host field formatting for the To header.
collector	Specifies the collector's host setting for formatting the Host field of the To header.
domain	Specifies the user defined domain name for formatting the Host field of the To header. The domain name is configure using the command *domain <name> on page 4949*.
user	Specifies the User field formatting for the Host field of the To header.
<*username*>	Specifies the user name used to format the User field of the To header.
none	Specifies that the user is not include in the Host field of the To header.

Default Values

By default, the host for formatting messages is **collector**, and the <*username*> is **collector.**

Command History

Release A2	Command was introduced.
Release R10.1.0	Command was added to the VQM Reporter command set.

Usage Examples

The following example sets the To header format to use the user defined domain name for formatting the To header:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#grammar to host domain**

The following example specifies that the user is not included in the User field of the To header:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#grammar to user none**

max-queue-depth *<value>*

Use the **max-queue-depth** command to specify the number of reports held in queue that are waiting to send requests or receive responses. Use the **no** form of this command to return the queue depth to the default value.

Syntax Description

<value>	Specifies the number of reports held in queue. Range is **0** to **2000**.

Default Values

By default, the reporter is configured to hold **512** reports in queue.

Command History

Release 17.6	Command was introduced.

Usage Examples

The following example sets the reporter to hold **700** reports in its queue:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#max-queue-depth 700**

max-retries *<value>*

Use the **max-retries** command to specify the number of times the reporter will attempt to contact the server. Use the **no** form of this command to return the number of attempts to the default value.

Syntax Description

<value>	Specifies the number of connection attempts. Range is **0** to **5**.

Default Values

By default, the voice quality monitoring (VQM) reporter is set to attempt to connect to the server **3** times.

Command History

Release 17.6	Command was introduced.

Functional Notes

After the reporter has attempted the maximum number of times to contact the server, the reports sent to the server are discarded. You can see how many reports have been discarded by using the command *debug ip security monitor on page 389*.

Usage Examples

The following example sets the number of connection attempts to **4**:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#max-retries 4**

outbound-proxy

Use the **outbound-proxy** command to specify the IP address or host name of the device receiving information from the voice quality monitoring (VQM) reporter before the information is sent to the collector. This command allows you to configure additional devices to receive VQM reporters in addition to a single collector. Using the **no** form of this command removes the outbound proxy server from the VQM reporter configuration. Variations of this command include:

outbound-proxy primary <*hostname* | *ip address*>
outbound-proxy primary <*hostname* | *ip address*> **tcp**
outbound-proxy primary <*hostname* | *ip address*> **tcp** <*port*>
outbound-proxy primary <*hostname* | *ip address*> **udp**
outbound-proxy primary <*hostname* | *ip address*> **udp** <*port*>
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*>
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*> **srv**
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*>
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*>
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv**
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
outbound-proxy primary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*> <*transport name prefix*>
outbound-proxy secondary <*hostname* | *ip address*>
outbound-proxy secondary <*hostname* | *ip address*> **tcp**
outbound-proxy secondary <*hostname* | *ip address*> **tcp** <*port*>
outbound-proxy secondary <*hostname* | *ip address*> **udp**
outbound-proxy secondary <*hostname* | *ip address*> **udp** <*port*>
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*>
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*> **srv**
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*>
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*>
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv**
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
outbound-proxy secondary <*hostname* | *ip address*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*> <*transport name prefix*>

Syntax Description

primary	Specifies this outbound proxy server as the primary contact server for the VQM reporter.
secondary	Specifies this outbound proxy server as the secondary contact server for the VQM reporter.

<hostname | ip address>	Specifies the host name or IP address of the outbound proxy. IP addresses should be expressed in the decimal dotted notation (for example, **10.10.10.1**).
tcp	Optional. Specifies that the reporter and outbound proxy server communicate using Transmission Control Protocol (TCP).
udp	Optional. Specifies that the reporter and outbound proxy server communicate using User Datagram Protocol (UDP).
tls *<profile name>*	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<port>	Optional. Specifies the port number used for communication between the reporter and the server. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<service name prefix>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<transport name prefix>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, no server is configured. When configured, by default, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release A4.03	Command was introduced.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Usage Examples

The following example specifies that the VQM reporter uses the outbound proxy server with the IP address of **172.5.67.99** as its **primary** server:

(config)**#ip rtp quality-monitoring reporter Reporter1**
(config-rtp-reporter-Reporter1)**#outbound-proxy primary 172.5.67.99**

The following example specifies the VQM collector as an outbound-proxy server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#ip rtp quality-monitoring reporter REPORTER1**
(config-rtp-reporter-REPORTER1)**#outbound-proxy primary 10.10.10.1 tls TLSPROFILE1**

VOICE TRUNKS COMMAND SETS

This section includes the following command sets:

VOICE ANALOG TRUNK COMMAND SET

Voice analog trunks are analog subscriber lines delivered by service providers that allow communication devices to connect to the outside world. To configure analog trunks, you must first configure the foreign exchange office (FXO) physical interface. By default, FXO interfaces are enabled, but their status must be verified before creating an analog trunk. For more information on configuring and verifying FXO interfaces, refer to the *FXO Interface Command Set on page 2364*.

Once the FXO interface is configured, a trunk account must be created for the analog trunk to make and receive calls. When creating trunk accounts, you must assign an FXO port to the trunk, and make sure the analog FXO settings (trunk number, supervision, etc.) match the parameters set by your service provider.

There are three main types of analog trunks supported by AOS. The first type is a dial pulse terminate (DPT) analog trunk, the second type is a loop start (LS) analog trunk, and the third is a ground start (GS) analog trunk. Configuration commands for all three analog trunk types are included in this section. For more information about configuring analog trunks, refer to the *NetVanta 7000 Series Trunk Accounts* configuration guide available online at https://supportcommunity.adtran.com.

To enter the Voice Analog Trunk DPT Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type analog supervision dpt
(config-t01)#
```

To enter the Voice Analog Trunk LS Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type analog supervision loop-start
(config-t01)#
```

To enter the Voice Analog Trunk GS Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type analog supervision ground-start
(config-t01)#
```

NOTE

*Not all Voice Analog Trunk commands apply to all analog trunk types. Use the **?** command to display a list of valid commands.*

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

alc on page 4962
anlp on page 4963
blind-dial on page 4964
busy all on page 4965
busy fxo <slot/port> on page 4966
busy-out monitor track <name> on page 4967
busy range fxo <range> on page 4968
caller-id on page 4969
caller-id-override on page 4970
codec-list <name> on page 4972
connect fxo <slot/port> on page 4974
connect range fxo <range> on page 4975
dialtone timeout <value> on page 4976
did digits-transferred <value> on page 4977
disconnect-supervision on page 4978
echo-cancellation on page 4979
loop-disconnect time <value> on page 4980
modem-passthrough on page 4981
plc on page 4982
prefer trunk-routing on page 4983
reject-external on page 4984
resource-selection on page 4985
rtp delay-mode on page 4986
rtp dtmf-relay on page 4987
rtp frame-packetization <value> on page 4988
rtp packet-delay on page 4989
rtp qos dscp <value> on page 4990
rtp rx-gain <value> on page 4991
rtp tx-gain <value> on page 4992
trunk-number <number> on page 4993

alc

Use the **alc** command to enable automatic level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature. Variations of this command include:

alc
alc level -16
alc level -17
alc level -18
alc level -19
alc level -20
alc level -21
alc level -22

Syntax Description

level -16	Optional. Specifies the ALC attenuation level is -16 dBm0.
level -17	Optional. Specifies the ALC attenuation level is -17 dBm0.
level -18	Optional. Specifies the ALC attenuation level is -18 dBm0.
level -19	Optional. Specifies the ALC attenuation level is -19 dBm0.
level -20	Optional. Specifies the ALC attenuation level is -20 dBm0.
level -21	Optional. Specifies the ALC attenuation level is -21 dBm0.
level -22	Optional. Specifies the ALC attenuation level is -22 dBm0.

Default Values

By default, ALC is disabled.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.
Release A2.04	Command was expanded to include the **level** parameters.

Usage Examples

The following example activates ALC on trunk **T01**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#alc**

anlp

Use the **anlp** command to enable advanced nonlinear processing which adds attenuation of residual echo level by way of a nonlinear processor (NLP) placed in the send path of an echo canceller. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **blind-dial** is disabled.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example enables anlp:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#anlp**

blind-dial

Use the **blind-dial** command to allow calls to be placed without the presence of dial tone. Use the **no** form of this command to disable blind dialing.

Syntax Description

No subcommands.

Default Values

By default, **blind-dial** is disabled.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example enables blind dialing:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#blind-dial**

busy all

Use the **busy all** command to set all level zero digital signals (DS0s) to busy so that no calls are allowed inbound or outbound. If any calls are active at the time this command is issued, the calls will stay active until either party terminates the call. Once terminated, the DS0s are busied out. Use the **no** form of this command to return to the default setting. Variations of this command include:

busy all
busy all now

Syntax Description

now	Optional. Immediately terminates calls that are active at the time the command is issued (for example, in the middle of a conversation).

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the analog voice trunk.

Usage Examples

The following example sets all DS0s on trunk **T01** to busy and terminates calls that are active at the time the command is issued:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#busy all now**

busy fxo <*slot/port*>

Use the **busy fxo** command to set a DS0 to busy so that no calls are allowed inbound or outbound. If a call is active at the time this command is issued, the call will stay active until either party terminates the call. Once terminated, the DS0 is set to busy. Use the **no** form of this command to disable this feature. Variations of this command include:

busy fxo <*slot/port*>
busy fxo <*slot/port*> **now**

Syntax Description

<*slot/port*>	Specifies the slot/port for the foreign exchange office (FXO).
now	Optional. Immediately terminates active call at the time the command is issued (for example, in the middle of a conversation).

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the analog voice trunk.

Usage Examples

The following example sets FXO 0/1 to busy and terminates an active call when the command is issued:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#busy fxo 0/1 now**

busy-out monitor track *<name>*

Use the **busy-out monitor track** command to automatically take a voice trunk out of service based on one or more conditions. The primary application of this feature is to signal to an attached private branch exchange (PBX) that because calls routed to the integrated access device (IAD) could fail due to loss of Session Initiation Protocoal (SIP) trunk connectivity, it should attempt to route the call via another interface. For more information on creating tracks, refer to *track <name> on page 1886* and the *Network Monitor Track Command Set on page 4098*. Use the no form of this command to remove a track from busy-out monitoring.

Syntax Description

<name>	Specifies the name of the track to monitor.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example shuts down trunk **T01** when the **on_fail** track fails:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#busy-out monitor track on_fail**

busy range fxo <*range*>

Use the **busy range fxo** command to set a particular set of level zero digital signals (DS0s) to busy so that no calls are allowed inbound or outbound. If any calls are active at the time this command is issued, the calls will stay active until either party terminates the call. Once terminated, the DS0s are set to busy. Use the **no** form of this command to return to the default setting. Variations of this command include:

busy range fxo <*range*>
busy range fxo <*range*> **now**

Syntax Description

<*range*>	Specifies a range of ports in the format <*slot/begin port range-end port range*> (for example, **0/1-4**).
now	Optional. Terminates calls that are active at the time the command is issued (for example, in the middle of a conversation).

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets DS0s to busy and terminates calls assigned to port range **fxo 0/1** through **fxo 0/4** when the command is issued:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#busy range fxo 0/1-4 now**

caller-id

Use the **caller-id** command to interpret and pass caller identification (ID) on this trunk. This information usually displays the name, number, time, and date of the calling party. Use the **no** form of this command to cancel the setting.

Syntax Description

No subcommands.

Default Values

By default, caller ID is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables caller ID:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#caller-id**

caller-id-override

Use the **caller-id-override** command to replace the calling party information for this trunk with a specific number. This command is used to conceal a user's name and number or to display a different name and number for internal or external caller ID. Use the **no** form of this command to cancel the setting. Variations of this command include:

caller-id-override emergency-outbound <*number*>
caller-id-override emergency-outbound match-substitute
caller-id-override name-inbound <*name*>
caller-id-override name-inbound <*name*> **if-unavailable**
caller-id-override number-inbound <*number*>
caller-id-override number-inbound <*number*> **if-no-cpn**
caller-id-override number-inbound <*number*> <*trunk id*>
caller-id-override privacy-outbound match-substitute

Syntax Description

emergency-outbound	Replaces the calling party number for outbound emergency calls.
<*number*>	Specifies the number to replace the calling party number for outbound emergency calls.
match-substitute	Specifies that the configured automatic number identification (ANI) match substitution is used for outbound emergency calls.
name-inbound <*name*>	Specifies the name to replace the calling party name for inbound calls.
if-unavailable	Specifies that the calling party name is replaced only if the calling party name is unavailable.
number-inbound <*number*>	Specifies the number to replace the calling party number for inbound calls.
<*trunk id*>	Optional. Specifies the trunk ID (**Txx**) for outbound calls.
if-no-cpn	Optional. Specifies that the calling party number is replaced only if the calling party number is unavailable.
privacy-outbound	Replaces the calling party number on anonymous outbound calls.
match-substitute	Specifies that the configured ANI match substitution is used for anonymous outbound calls.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 15.1	Command was expanded.
Release 16.1	Command was expanded to include the **if-no-cpn** parameter.
Release A4.01	Command was expanded to include the **match-substitute** parameter.
Release R11.8.0	Command was expanded to include the **privacy-outbound** parameter.

Usage Examples

The following example sets the caller ID override number on the trunk where the command is issued:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#caller-id-override number-inbound 555-8000**

codec-list *<name>*

Use the **codec-list** command to specify the coder-decoder (CODEC) list to be used by this account. This CODEC can be used for normal voice traffic or for Session Border Controller (SBC) transcoding. Use the **no** form of this command to remove the CODEC list from the account. Variations of this command include:

codec-list *<name>*
codec-list *<name>* **both**
codec-list *<name>* **in**
codec-list *<name>* **out**
codec-list any
codec-list any both
codec-list any in
codec-list any out

Syntax Description

<name>	Specifies the CODEC list to be used for this account.
any	Specifies that any possible CODEC is allowed on this account.
both	Optional. Specifies that the CODEC list is applied to both transmitted and received Session Description Protocol (SDP) transmissions.
in	Optional. Specifies that the CODEC list is applied to received SDP only.
out	Optional. Specifies that the CODEC list is applied to transmitted SDP only.

Default Values

By default, no CODEC lists are assigned.

Command History

Release R10.4.0	Command was introduced and replaced the **codec-group** command.

Functional Notes

The **codec-list** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893***.**

In addition, CODEC lists can be used for the SBC transcoding feature. For more information about this feature, its uses, and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

> NOTE *Because you can choose to specify that any CODEC is used by a Session Initiation Protocol (SIP) endpoint with the **any** keyword, do not create a CODEC list with the name of **any**.*

Usage Examples

The following example applies the CODEC list **LIST1** to incoming SDP traffic on trunk **T01**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#codec-list LIST1 in**

connect fxo *<slot/port>*

Use the **connect fxo** command to specify the physical interface this trunk will use for voice calls. Use the **no** form of this command to remove this association.

Syntax Description

<slot/port>	Specifies the slot/port for the foreign exchange office (FXO) trunk.

Default Values

By default, no physical interface is assigned.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the analog voice trunk.

Usage Examples

The following example specifies this trunk to use port **fxo 0/1**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#connect fxo 0/1**

connect range fxo <*range*>

Use the **connect range fxo** command to specify the range of physical interfaces for this trunk group usage. Use the **no** form of this command to return to the default setting.

Syntax Description

<*range*>	Specifies a range of ports in the format <*slot/begin port range-end port range*> (for example, **0/1-4**).

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies that this analog loop start (LS) trunk will use the contiguous port range **fxo 0/1** through **fxo 0/4**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#connect range fxo 0/1-4**

dialtone timeout *<value>*

Use the **dialtone timeout** command to specify the dial tone detection timeout period (in milliseconds) for dial tone detection.

Syntax Description

<value>	Specifies the dial tone detection timeout period in milliseconds. Valid rage is **1500** to **60000** milliseconds.

Default Values

By default, the dial tone detection timeout period is **2000** milliseconds for the United States, Puerto Rico, and Canada and is **4000** milliseconds for all other supported countries.

Command History

Release A4.05	Command was introduced.

Usage Examples

The following example specifies that analog loop start trunk **t01** will use a **3000** milliseconds dial tone detection timeout period:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#dialtone timeout 3000**

did digits-transferred <*value*>

Use the **did digits-transferred** command to define how many of the received digits should be sent to the internal switchboard from an incoming call on a user role trunk. The number of digits transferred are the least significant digits received. Direct inward dialing (DID) should be used if a Telco provider is providing digits to the unit on inbound calls or if the unit needs to provide DID information to a piece of customer premises equipment (CPE). Use the **no** form of this command to disable this feature. Variations of this command include:

did digits-transferred <*value*>
did digits-transferred <*value*> **prefix** <*number*>

Syntax Description

<*value*>	Specifies the number of digits to be transferred. Range is **1** to **16** digits.
prefix <*number*>	Optional. Specifies a sequence of digits to be prepended to the digits that will be transmitted. For example, if seven digits will be transferred via DID, then prefix the seven digits with 256. Thus, **555-8000** would be prefixed with **256**, transmitting out the string of digits **256-555-8000**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Functional Notes

User Role Example:

555-1000 is an incoming call on the trunk. With **did digits-transferred** <*value*> set to 4, the number 1000 will be sent to the switchboard. On a network role trunk, the **did digits-transferred** command allows you to define how many of the digits from the Accept criteria should be sent externally from a call that was routed by the switchboard. The number of digits transferred are the least significant digits received.

Network Role Example:

555-1000 is accepted on the universal time (UT) interface. With **did digits-transferred** <*value*> set to 4, the number of 1000 will be sent to the device connected to the UT interface. This command cannot be specified if and when **trunk-number** is being used. Conversely, if DID is used, **trunk-number** will not be allowed.

Usage Examples

The following example transfers the digits **555-8000** and adds the prefix **256**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#did digits-transferred 5558000 prefix 256**

disconnect-supervision

Use the **disconnect-supervision** command to configure disconnect supervision for calls on the analog voice trunk. Use the **no** version of this command to disable this feature. Variations of this command include:

disconnect-supervision release-delay <*seconds*>
disconnect-supervision tone busy
disconnect-supervision tone busy <*seconds*>

Syntax Description

release-delay <*seconds*>	Specifies the time delay (in seconds) between when the call is terminated and when the unit places the FXO port in an idle state. Range is **1** to **120** seconds.
tone busy	Specifies that the voice trunk be monitored for busy tone. Upon detection of busy tone, the call will be disconnected after **10** seconds.
<*seconds*>	Specifies the time delay (in seconds) between the busy tone detection and the termination of the call. Range is **1** to **120** seconds.

Default Values

By default, **disconnect-supervision** is disabled.

Command History

Release A4.05	Command was introduced.
Release R10.2.0	Command was expanded to include the **release-delay** parameter.

Functional Notes

Disconnect supervision monitors a foreign exchange office (FXO) port for a specific condition to determine when the line should be released. Disconnect supervision is used in auto attendant, fax, and modem applications to ensure that a connection is not maintained indefinitely when a call has ended or could not be completed.

Usage Examples

The following example enables disconnect supervision for busy tone:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#disconnect-supervision tone busy**

echo-cancellation

Use the **echo-cancellation** command to improve voice quality for packetized-based voice calls, such as Voice over Internet Protocol (VoIP) or Media Gateway Control Protocol (MGCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **echo-cancellation** is enabled.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example activates **echo-cancellation**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#echo-cancellation**

loop-disconnect time <*value*>

Use the **loop-disconnect time** command to specify the length of time a line must maintain a loop current feed open (LCFO) state to qualify as a valid disconnection. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

The default loop-disconnect time is determined using the command *voice system-country <name> on page 1970*. The list below shows the default loop disconnect time (in milliseconds) for fully-supported countries:

Australia	500 ms	Mexico	500 ms
Belgium	200 ms	Puerto Rico	500 ms
Canada	500 ms	United Arab Emirates	200 ms
ETSI	200 ms	United Kingdom	200 ms
Ireland	200 ms	United States	500 ms

Command History

Release A5.01	Command was introduced.

Functional Notes

Loop disconnect time is only configurable on ground start and loop start analog trunks.

Usage Examples

The following example configures the loop disconnect time for loop start trunk T01 as **500** ms:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#loop-disconnect time 500**

modem-passthrough

Use the **modem-passthrough** command to switch to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings, such as echo cancellation and voice activity detection (VAD). Use the **no** form of this command to disable this feature. Variations of this command include:

modem-passthrough
modem-passthrough detection-time <*value*>
modem-passthrough cng-early-detect

Syntax Description

detection-time <*value*>	Optional. Specifies the fax and/or modem detection time length value in seconds. Range is **0** to **8** seconds.
cng-early-detect	Optional. Enables early (first burst) detection of fax calling (CNG) tone.

Default Values

By default, **modem-passthrough** is enabled.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command was expanded.
Release R10.8.0	Command was expanded to include the **cng-early-detect** parameter.

Usage Examples

The following example disables **modem-passthrough**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#no modem-passthrough**

plc

Use the **plc** command to enable packet loss concealment (PLC). PLC is used to prevent choppy connections by concealing a packet loss by replacing the lost packet with another voice packet in the data stream. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, PLC is enabled on this interface.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example disables PLC on trunk **T01**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#no plc**

prefer trunk-routing

Use the **prefer trunk-routing** command to add a trunk to a list of trunks that are considered first for call routing, regardless of system routing mode or locally configured extensions. Use the **no** form of this command to remove the trunk from the list.

Syntax Description

No subcommands.

Default Values

By default, **prefer trunk-routing** is disabled.

Command History

Release A2	Command was introduced.

Functional Notes

Trunk routing can be specified as a preference for specific trunks, allowing the trunk to be considered first for routing rather than relying on the internal or external nature of the call to dictate whether the trunk or voice station is the first choice routing path. The **prefer trunk-routing** command, executed from a specific trunk's configuration mode, adds the trunk to a list of trunks that are considered first for routing.

By default, no trunk routing preference is set, so that each trunk operates as dictated by normal call routing modes. Adding the trunk routing preference only affects how inbound calls from the specific trunk are handled.

Usage Examples

The following example specifies that trunk routing is preferred on the trunk **T01**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#prefer trunk-routing**

reject-external

Use the **reject-external** command to prevent inbound calls on the trunk from being routed back out of the same trunk. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **reject-external** is enabled on this interface.

Command History

Release 9.3	Command was introduced.

Functional Notes

In general, trunks are assigned to the user role, which means they terminate lines from a Telco provider. If this is the case, **reject-external** should be enabled so that inbound calls on the trunk cannot be routed back out of the same trunk. If the configuration is poor, inbound long distance calls could be routed back out the same trunk, causing the owner of the unit to be charged for long distance calls without his knowledge. For network-role trunks and Session Initiation Protocol (SIP) based trunks, this command should be disabled to allow calls to be properly routed in the unit.

Usage Examples

The following example disables **reject-external**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#no reject-external**

resource-selection

Use the **resource-selection** command to determine how the switchboard uses outbound call resources contained within a time division multiplexing (TDM) based trunk group. Use the **no** form of this command to disable this feature. Variations of this command include:

resource-selection circular
resource-selection circular ascending
resource-selection circular descending
resource-selection linear
resource-selection linear ascending
resource-selection linear descending

Syntax Description

circular	Performs call load balancing among available DS0s/B-channels in this trunk. Subsequent calls will be delivered to the next available DS0/B-channel in a round-robin fashion.
linear	Specifies that a call being delivered to this trunk will be accepted out the first available DS0/B-channel available at the time the call is received.
ascending	Optional. Distributes calls in an order from the lowest to the highest channel (DS0 1, 2, 3 through 24).
descending	Optional. Distributes calls in an order from the highest to the lowest channel (DS0 24, 23, 22 through 1).

Default Values

By default, resource selection is set to **linear**.

Command History

Release 9.3	Command was introduced.
Release 13.1	Command was expanded to include the **ascending** and **descending** subcommands.

Usage Examples

The following example specifies circular resource selection:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#resource-selection circular**

rtp delay-mode

Use the **rtp delay-mode** command to configure the Realtime Transport Protocol (RTP) jitter buffer packet delay mode settings. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Use the **no** form of this command to return to the default setting. Variations of this command include:

rtp delay-mode adaptive
rtp delay-mode fixed

Syntax Description

adaptive	Configures the RTP jitter buffer packet delay to adjust during a call based on network conditions.
fixed	Configures the RTP jitter buffer packet delay to remain constant.

Default Values

By default, the RTP delay mode is set to **adaptive**. This allows for minimal latency by adjusting the average packet delay based on the conditions of the network.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures RTP delay mode as **fixed**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#rtp delay-mode fixed**

rtp dtmf-relay

Use the **rtp dtmf-relay** command to configure the method by which Realtime Transport Protocol (RTP) dual tone multi-frequency (DTMF) events are relayed. The dial digits can be sent inband or out-of-band (OOB) of the voice stream. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp dtmf-relay inband
rtp dtmf-relay nte <*value*>

Syntax Description

inband	Specifies that RTP DTMF events be relayed inband in the RTP stream.
nte <*value*>	Specifies that RTP DTMF events be relayed OOB using named telephone event (NTE). Enter an NTE value between **96** and **127**.

Default Values

By default, the **rtp dtmf-relay** is set for **NTE 101**.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example configures RTP DTMF relay events for **inband**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#rtp dtmf-relay inband**

rtp frame-packetization <*value*>

Use the **rtp frame-packetization** command to configure the Realtime Transport Protocol (RTP) frame packetization time in milliseconds for individual trunks and users. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP frame packetization time value in milliseconds. Select from **10**, **20**, **30**, or **40** milliseconds.

Default Values

By default, the **rtp frame-packetization** time is set to **20** milliseconds on all trunks and users.

Command History

Release 9.3	Command was introduced.
Release R10.8.0	Command was expanded to include **40** milliseconds.

Usage Examples

The following example sets the frame packetization time for trunk **T01** to **10** milliseconds:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#rtp frame-packetization 10**

rtp packet-delay

Use the **rtp packet-delay** command to configure the maximum Realtime Transport Protocol (RTP) packet delays. This command is used to set the allowable limits of latency on the network. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp packet-delay fax <*value*>
rtp packet-delay maximum <*value*>
rtp packet-delay nominal <*value*>

Syntax Description

fax <*value*>	Sets the fax delay time value. Range is **0** to **500** milliseconds.
maximum <*value*>	Sets the maximum delay time value in increments of **10** milliseconds. Range is **40** to **320** milliseconds.
nominal <*value*>	Sets the nominal delay time value in increments of **10** milliseconds. Range is **10** to **240** milliseconds.

Default Values

By default, the RTP packet delay for fax is **300**, maximum is **100**, and nominal is **50**.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the RTP fax delay time on trunk **T01** to **200** milliseconds:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#rtp packet-delay fax 200**

rtp qos dscp <*value*>

Use the **rtp qos dscp** command to configure the maximum Realtime Transport Protocol (RTP) quality of service (QoS) parameters for differentiated services code point (DSCP). Use the **no** form of this command to return to the default global value.

Syntax Description

<*value*>	Configures the RTP QoS parameter for DSCP. Enter a value between **0** and **63**.

Default Values

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. The default global DSCP value for RTP is **46**.

Command History

Release 9.3	Command was introduced.

Functional Notes

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. QoS is set using a DSCP value. Valid DSCP values are **0** to **63**, and a higher DSCP value has a higher priority. The default global DSCP value for RTP is **46**. Remember that if you are using a public IP connection, such as the Internet, for Voice over Internet Protocol (VoIP), end-to-end QoS may not be guaranteed. The default DSCP value for Session Initiation Protocol (SIP) is **26**. To configure QoS for the RTP traffic that carries the voice conversation, use the command **ip rtp qos dscp** followed by the desired DSCP value.

Usage Examples

The following example configures the RTP QoS DSCP for trunk **T02** to **60**:

(config)**#voice trunk t02 type analog supervision loop-start**
(config-t02)**#rtp qos dscp 60**

rtp rx-gain *<value>*

Use the **rtp rx-gain** command to specify the Realtime Transport Protocol (RTP) receive (RX) gain or attenuation. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Using the **no** form of this command returns the RTP RX gain or attenuation to the default value.

Syntax Description

<value>	Specifies the RTP RX gain or attenuation in the RTP to time division multiplexing (TDM) direction. Range is **6** to **-14**. Negative values specify attenuation. Positive values specify gain in decibels (dB).

Default Values

By default, RTP RX gain is set to **0** dB.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies the RTP RX gain for trunk **T01** is **4** dB:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#rtp rx-gain 4**

rtp tx-gain <*value*>

Use the **rtp tx-gain** command to specify the Realtime Transport Protocol (RTP) transmit (TX) gain or attentuation. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Using the **no** form of this command returns the RTP TX gain or attenuation to the default value.

Syntax Description

<*value*>	Specifies the RTP TX gain or attenuation in the time division multiplexing (TDM) to RTP direction. Range is **6** to **-14**. Negative values specify attenuation. Positive values specify gain in decibels (dB).

Default Values

By default, RTP TX gain is set to **0** dB.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies the RTP TX gain for trunk **T01** is **4** dB:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#rtp tx-gain 4**

trunk-number <*number*>

Use the **trunk-number** command to define the call routing when direct inward dialing (DID) is disabled. This feature directs incoming calls to the specified number when DID is not present. This command also allows users to activate different system modes of operation that redirect incoming calls to a different number depending on the specified mode. Use the **no** form of this command to disable this feature. Variations of this command include:

trunk-number <*number*>
trunk-number no-number
trunk-number <*system mode*> <*number*>
trunk-number <*system mode*> **no-number**
trunk-number override <*number*>
trunk-number override no-number

Syntax Description

<*number*>	Specifies the number used for call routing when DID is disabled.
<*system mode*>	Optional. Specifies the system mode to configure. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the command *voice system-mode on page 1971* for more information on system modes.
no-number	Specifies no inbound calls are allowed on this trunk.
override	Ignores the programmed system mode schedule.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the feature group D (FGD) trunk options.
Release A1	Command was expanded to include the new subcommands.

Usage Examples

The following example defines call routing on trunk **T03**:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#trunk-number 4000**

t38

Use the **t38** command to enable T.38 fax operation. Use the **no** form of this command to disable this feature.

The command modem-passthrough on page 4981 must be enabled for T.38 operation to work.

Syntax Description

No subcommands.

Default Values

By default, T.38 is disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables T.38 on trunk **T01**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38**

Technology Review

T.38 is an International Telecommunication Union (ITU) specification that allows Group-3 Fax (T.30) data to be transported over the Internet. It is similar to dual tone multi-frequency (DTMF) relay (RFC 2833) in that the digital signal processor (DSP) decodes tones and demodulated fax data and converts them into packets. A similar device on the other end takes the packets/tones and remodulates them so that an analog fax machine on the other end can receive the fax. AOS's previous support (revisions 12 through 15) for fax/modem signals was simply detecting a tone and forcing the coder-decoder (CODEC) into G.711 and disabling/enabling echo cancellers based on the tones detected. When packet loss becomes high, sending faxes over G.711 becomes problematic, due to dropped messages and timeouts/retrains.

T.38 can be used in conjunction with various call-control schemes, such as H.323, Session Initiation Protocol (SIP), and Media Gateway Control Protocol (MGCP). AOS only supports SIP as the call-control method. This is typically referred to T.38/Annex-D. Annex-D describes the Session Initiation Protocol/Session Description Protocol (SIP/SDP) call establishment procedures.

t38 ced auto-generate

Use the **t38 ced auto-generate** command to specify when the digital signal processor (DSP) should regenerate the called station identifier (CED) signal toward the time division multiplexed (TDM) endpoint. If auto-generate is enabled, the DSP generates the CED signal only when it does not receive CED indicator packets from the Voice over IP (VoIP) endpoint. If auto-generate is disabled, the DSP generates the CED signal only when it does receive CED indicator packets from the VoIP endpoint. Using the **no** version of this command disables CED auto-generate.

Syntax Description

No subcommands.

Default Values

By default, CED auto-generate is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example enables CED auto-generate for the T.38 session on the trunk:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 ced auto-generate**

t38 ced length <*time*>

Use the **t38 ced length** command to set the maximum duration of a regenerated called station identifier (CED) signal, in milliseconds, from the digital signal processor (DSP) toward the time division multiplexed (TDM) endpoint when a T.38 session is active. Using the **no** form of this command returns the duration to the default value.

Syntax Description

<time>	Specifies the maximum duration of a regenerated CED signal in milliseconds. Valid range is **0** to **4000** ms.

Default Values

By default, the maximum duration of a regenerated CED signal is **3000** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Setting the maximum duration of a regenerated CED signal to **0** effectively prevents any CED generation.

Usage Examples

The following example decreases the maximum duration of the CED signal to **2000** ms for the T.38 session:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 ced length 2000**

t38 cng-relay-selective

Use the **t38 cng-relay-selective** command to enable fax calling tones (CNG) relay only when V.21 messages are not being transmitted. Use the **no** version of this command to disable selective CNG relay.

Syntax Description

No subcommands.

Default Values

Selective CNG relay is disabled by default.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables T.38 CNG relay:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 cng-relay-selective**

t38 ecm

Use the **t38 ecm** command to enable or disable error correction mode (ECM) during T.38 sessions. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 ecm enable
t38 ecm disable

Syntax Description

enable	Enables ECM during T.38 sessions.
disable	Disables ECM during T.38 sessions.

Default Values

By default, ECM is enabled.

Command History

Release R10.8.0	The command was introduced

Usage Examples

The following example disables ECM for T.38 sessions on trunk T01:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 ecm disable**

t38 error-correction

Use the **t38 error-correction** command to specify the type of fax error correction. Use the **no** form of this command to disable this feature. Variations of this command include:

t38 error-correction fec
t38 error-correction redundancy

Syntax Description

fec	Specifies forward error correction (FEC) as the fax error correction. FEC is a system of error control where the sender adds redundant data to its messages, allowing the receiver to detect and correct errors (within certain bounds) without the need to request additional data from the sender.
redundancy	Specifies redundancy as the fax error correction. Redundancy error correction replicates the payload a user-specified number of times to determine if errors are present. The number of redundant packets is set using the command *t38 v21-preamble-timeout <value> on page 5006*).

Default Values

By default, **t38 error-correction** is set to **redundancy** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, the NetVanta 6240/6250 Serires, and the NetVanta 640 Series.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default value changed to **fec** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, and the NetVanta 7000 Series products.
Release R10.8.0	The default values for this command were updated.

Usage Examples

The following example sets the **t38 error-correction** to **fec**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 error-correction fec**

t38 fallback-mode g711

Use the **t38 fallback-mode** command to specify the transmission mode used when T.38 fax relay cannot be successfully negotiated at the time of the fax transfer. Use the **no** form of this command to disable this feature.

Syntax Description

g711	Specifies that fax operation revert back to analog mode (G.711).

Default Values

By default, **t38 fallback-mode** is to **G.711**.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **G.711**.

Usage Examples

The following example enables the **t38 fallback-mode** on trunk **T02**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 fallback-mode g711**

t38 generate-cng

Use the **t38 generate-cng** command to specify whether the digital signal processor (DSP) will begin a T.38 session by generating the calling signal (CNG) toward the time division multiplexed (TDM) endpoint. Using the **no** version of this command disables CNG generation.

Syntax Description

No subcommands.

Default Values

By default, CNG generation is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

With the introduction of this command, the CNG generation behavior of the T.38 session is now configurable. In AOS firmware prior to A5.01, this behavior was not configurable, but rather was set to always generate this signal.

Usage Examples

The following example enables CNG generation for the T.38 session:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 generate-cng**

t38 max-buffer <*value*>

Use the **t38 max-buffer** command to set the maximum buffer size for T.38 fax operation. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-buffer** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **800** bytes.

Default Values

By default, the maximum buffer size is set to **200**.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-buffer** to **100**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 max-buffer 100**

t38 max-datagram <*value*>

Use the **t38 max-datagram** command to set the maximum datagram value in this unit. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-datagram** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **300** bytes.

Default Values

By default, the maximum datagram value is set to **72** bytes.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **72** bytes.

Usage Examples

The following example sets the **t38 max-datagram** to **100**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 max-datagram 100**

t38 max-rate

Use the **t38 max-rate** command to specify the fax maximum rate. The actual transmission rate could be lower than specified rate if the receiving end cannot support the maximum rate. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 max-rate 14400
t38 max-rate 12000
t38 max-rate 2400
t38 max-rate 4800
t38 max-rate 7200
t38 max-rate 9600

Syntax Description

14400	Specifies 14400 bits per second (bps) as fax maximum rate.
12000	Specifies 12000 bps as fax maximum rate.
2400	Specifies 2400 bps as fax maximum rate.
4800	Specifies 4800 bps as fax maximum rate.
7200	Specifies 7200 bps as fax maximum rate.
9600	Specifies 9600 bps as fax maximum rate.

Default Values

By default, the maximum fax rate is set to **14400** bps.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-rate** to **4800** bps:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 max-rate 4800**

t38 redundancy

Use the **t38 redundancy** command to set the number of redundant packets sent when the **t38 error-correction redundancy** feature is enabled. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 redundancy high-speed <*value*>
t38 redundancy low-speed <*value*>

Syntax Description

high-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for data messages (high-speed fax machine image data). Range is **0** (no redundancy) to **4** packets.
low-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for the signaling messages (low-speed fax machine protocol). Range is **0** (no redundancy) to **7** packets.

Default Values

By default, high-speed and low-speed redundancy values are set to **0** (no redundancy).

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables **t38 error-correction redundancy** and sets the number of redundant data messages to **3** on trunk **T01**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 error-correction redundancy**
(config-t01)**#t38 redundancy high-speed 3**

t38 v21-preamble-timeout *<value>*

Use the **t38 v21-preamble-timeout** command to set the maximum amount of time that the digital signal processor (DSP) waits for peer device activity after starting to transmit a V.21 preamble event before spoofing a response to the time division multiplexed (TDM) endpoint. Using the **no** version of this command returns the timeout value to the default setting.

Syntax Description

<value>	The time, in milliseconds, that the DSP will wait for peer activity. Valid range is **1** to **3000** ms.

Default Values

By default, the V.21 preamble timeout is set to **1700** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example specifies the V.21 preamble timeout value as **2000** ms:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#t38 v21-preamble-timeout 2000**

vad

Use the **vad** command to enable voice activity detection (VAD). VAD blocks out noise categorized as silence during a voice connection. The silent voice packets are not transmitted, allowing bandwidth usage to be reduced. Although VAD saves bandwidth, the quality of the voice call may be compromised. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, VAD is enabled for all T1 robbed bit signaling (RBS) trunks and users.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example disables VAD on trunk **T01**:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#no vad**

VOICE ISDN TRUNK COMMAND SET

The integrated services digital network (ISDN) primary rate interface (PRI) is a circuit composed of 23 bearer (B) channels and 1 data (D) channel. ISDN PRI is an international standard for digital communications, allowing a full range of enhanced services supporting voice and data. The 23 B channels are used to transmit voice or data over an all-digital public switched telephone network (PSTN). The D channel is used to transmit out-of-band (OOB) signaling for the B channels and controls dialing numbers and features such as call waiting.

Voice ISDN trunks are digital subscriber lines delivered by service providers that connect communication devices through the PRI interface to the outside world. In order to configure ISDN trunks, you must configure a trunk account to make and receive calls. To do this, you create a trunk account (using the command *voice trunk <trunk id> type on page 1980*) and assign the PRI interface (using the command *cross-connect on page 76*). When you configure the trunk account, make sure the PRI settings (trunk number, caller ID, etc.) match the parameters set by your service provider. For more information about the creation and use of ISDN trunks, refer to the *Total Access 900 Series ISDN PRI Interface* quick configuration guide or the *NetVanta 7000 Series Trunk Accounts* configuration guide available online at https://supportcommunity.adtran.com.

To create an ISDN trunk account and enter the Voice ISDN Trunk Configuration mode, enter **voice trunk** *<trunk id>* **type isdn** at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type isdn
(config-t01)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

alc on page 5010
caller-id-override on page 5011
codec-list <name> on page 5013
connect isdn-group <number> on page 5015
early-cut-through on page 5016
echo-cancellation on page 5017
match ani <template> substitute <template> on page 5018
match dnis <template> replace ani <number> on page 5020

alc

Use the **alc** command to enable automatic level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature. Variations of this command include:

alc
alc level -16
alc level -17
alc level -18
alc level -19
alc level -20
alc level -21
alc level -22

Syntax Description

level -16	Optional. Specifies the ALC attenuation level is -16 dBm0.
level -17	Optional. Specifies the ALC attenuation level is -17 dBm0.
level -18	Optional. Specifies the ALC attenuation level is -18 dBm0.
level -19	Optional. Specifies the ALC attenuation level is -19 dBm0.
level -20	Optional. Specifies the ALC attenuation level is -20 dBm0.
level -21	Optional. Specifies the ALC attenuation level is -21 dBm0.
level -22	Optional. Specifies the ALC attenuation level is -22 dBm0.

Default Values

By default, ALC is disabled.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.
Release A2.04	Command was expanded to include the **level** parameters.

Usage Examples

The following example activates the ALC for the trunk:

(config)**#voice trunk t01 type isdn**
(config-t01)**#alc**

caller-id-override

Use the **caller-id-override** command to replace the calling party information for this trunk with a specific number. This command is used to conceal a user's name and number or to display a different name and number for internal or external caller ID. Use the **no** form of this command to cancel the setting. Variations of this command include:

caller-id-override emergency-outbound <*number*>
caller-id-override emergency-outbound match-substitute
caller-id-override name-inbound <*name*>
caller-id-override name-inbound <*name*> **if-unavailable**
caller-id-override number-inbound <*number*>
caller-id-override number-inbound <*number*> **if-no-cpn**
caller-id-override number-inbound <*number*> <*trunk id*>
caller-id-override privacy-outbound match-substitute

Syntax Description

emergency-outbound	Replaces the calling party number for outbound emergency calls.
<*number*>	Specifies the number to replace the calling party number for outbound emergency calls.
match-substitute	Specifies that the configured automatic number identification (ANI) match substitution is used for outbound emergency calls.
name-inbound <*name*>	Specifies the name to replace the calling party name for inbound calls.
if-unavailable	Specifies that the calling party name is replaced only if the calling party name is unavailable.
number-inbound <*number*>	Specifies the number to replace the calling party number for inbound calls.
<*trunk id*>	Optional. Specifies the trunk ID (**Txx**) for outbound calls.
if-no-cpn	Optional. Specifies that the calling party number is replaced only if the calling party number is unavailable.
privacy-outbound	Replaces the calling party number on anonymous outbound calls.
match-substitute	Specifies that the configured ANI match substitution is used for anonymous outbound calls.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 15.1	Command was expanded.
Release 16.1	Command was expanded to include the **if-no-cpn** parameter.
Release A4.01	Command was expanded to include the **match-substitute** parameter.
Release R11.8.0	Command was expanded to include the **privacy-outbound** parameter.

Usage Examples

The following example sets the caller ID override number on the trunk where the command is issued:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#caller-id-override number-inbound 555-8000**

codec-list *<name>*

Use the **codec-list** command to specify the coder-decoder (CODEC) list to be used by this account. This CODEC can be used for normal voice traffic or for Session Border Controller (SBC) transcoding. Use the **no** form of this command to remove the CODEC list from the account. Variations of this command include:

codec-list *<name>*
codec-list *<name>* **both**
codec-list *<name>* **in**
codec-list *<name>* **out**
codec-list any
codec-list any both
codec-list any in
codec-list any out

Syntax Description

<name>	Specifies the CODEC list to be used for this account.
any	Specifies that any possible CODEC is allowed on this account.
both	Optional. Specifies that the CODEC list is applied to both transmitted and received Session Description Protocol (SDP) transmissions.
in	Optional. Specifies that the CODEC list is applied to received SDP only.
out	Optional. Specifies that the CODEC list is applied to transmitted SDP only.

Default Values

By default, no CODEC lists are assigned.

Command History

Release R10.4.0	Command was introduced and replaced the **codec-group** command.

Functional Notes

The **codec-list** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893***.**

In addition, CODEC lists can be used for the SBC transcoding feature. For more information about this feature, its uses, and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

> NOTE *Because you can choose to specify that any CODEC is used by a Session Initiation Protocol (SIP) endpoint with the **any** keyword, do not create a CODEC list with the name of **any**.*

Usage Examples

The following example applies the CODEC list **LIST1** to incoming SDP traffic on trunk **T01**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#codec-list LIST1 in**

connect isdn-group <*number*>

Use the **connect isdn-group** command to associate a trunk with an integrated services digital network (ISDN) group. The ISDN group number uniquely identifies an ISDN trunk group. Use the **no** form of this command to remove this association.

Syntax Description

<*number*>	Specifies the ISDN group number. Range is **1** to **255**.

Default Values

By default, no group is defined.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the ISDN trunk.

Usage Examples

The following example specifies that this trunk will use the ISDN group **1**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#connect isdn-group 1**

early-cut-through

Use the **early-cut-through** command to provide the caller with inband ringback and other call progress signals. This command should not be issued if the connected equipment does not provide inband ringback and other call progress signals. This option is only valid for voice trunks in the network role. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **early-cut-through** is enabled.

Command History

Release A5.02	Command was introduced.

Usage Examples

The following example disables early-cut-through:

```
(config)#voice trunk t01 type isdn
(config-t01)#no early-cut-through
```

echo-cancellation

Use the **echo-cancellation** command to improve voice quality for packetized-based voice calls, such as Voice over IP (VoIP) or Media Gateway Control Protocol (MGCP). Enabling this command may significantly improve the voice quality in calls across the telephone network. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **echo-cancellation** is enabled.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the integrated services digital network (ISDN) trunk.

Usage Examples

The following example activates **echo-cancellation**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#echo-cancellation**

match ani <*template*> substitute <*template*>

Use the **match ani substitute** command to configure automatic number identification (ANI) substitution for outbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

match ani <*template*> **substitute** <*template*>
match ani <*template*> **substitute** <*template*> **name** <*name*>

Syntax Description

ani <*template*>	Specifies the ANI information to be substituted. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the ANI information that is substituted for the original ANI information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
name <*name*>	Optional. Specifies the name associated with the ANI information. This option is only available on trunks that support ANI name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no ANI substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for ANI templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the ANI information from numbers **555-8111** to **555-8115** will be substituted by **555-8110** for outbound calls on the trunk **T03**:

(config)**#voice trunk t03 type isdn**
(config-t03)**#match ani 555-811[125] substitute 555-8110**

match dnis <*template*> replace ani <*number*>

Use the **match dnis replace ani** command to replace dialed number identification service (DNIS) information with automatic number identification (ANI) information on outbound voice trunks. Use the **no** form of this command to remove the replacement. Variations of this command include:

match dnis <*template*> **replace ani** <*number*>
match dnis <*template*> **replace ani** <*number*> **name** <*name*>

Syntax Description

dnis <*template*>	Specifies the DNIS information to be replaced. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
replace ani <*number*>	Specifies the ANI information that replaces the original DNIS information. This information is entered using numerical digits. Enter the number without punctuation.
name <*name*>	Optional. Specifies the name associated with the ANI information. This option is only available on trunks that support ANI name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no DNIS replacement is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for DNIS templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits

3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the DNIS information for dialed numbers on trunk **T03** that match **1-256-524-8600** are replaced with **882-6467**:

(config)**#voice trunk t03 type isdn**
(config-t03)**#match dnis 1-256-524-8600 replace ani 8826467**

match dnis <*template*> substitute <*template*>

Use the **match dnis substitute** command to configure dialed number identification service (DNIS) substitution for outbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

match dnis <*template*> **substitute** <*template*>
match dnis <*template*> **substitute** <*template*> **name** <*name*>

Syntax Description

dnis <*template*>	Specifies the DNIS information to be substituted. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the DNIS information that is substituted for the original DNIS information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
name <*name*>	Optional. Specifies the name associated with the DNIS information. This option is only available on trunks that support DNIS name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no DNIS substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for DNIS templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the DNIS information for dialed numbers on trunk **T03** that match **1-334-NXX-XXXX** are substituted with **1-800-557-4500**:

(config)**#voice trunk t03 type isdn**
(config-t03)**#match dnis 1-334-NXX-XXXX substitute 1-800-557-4500**

modem-passthrough

Use the **modem-passthrough** command to switch to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings, such as echo cancellation and voice activity detection (VAD). Use the **no** form of this command to disable this feature. Variations of this command include:

modem-passthrough
modem-passthrough detection-time <*value*>
modem-passthrough cng-early-detect

Syntax Description

detection-time <*value*>	Optional. Specifies the fax and/or modem detection time length value in seconds. Range is **0** to **8** seconds.
cng-early-detect	Optional. Enables early (first burst) detection of fax calling (CNG) tone.

Default Values

By default, **modem-passthrough** is enabled.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command was expanded.
Release R10.8.0	Command was expanded to include the **cng-early-detect** parameter.

Usage Examples

The following example enables **modem-passthrough**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#modem-passthrough**

plc

Use the **plc** command to enable packet loss concealment (PLC). PLC is used to prevent choppy connections by concealing a packet loss by replacing the lost packet with another voice packet in the data stream. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, PLC is enabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables PLC on trunk **T01**:

```
(config)#voice trunk t01 type isdn
(config-t01)#plc
```

prefer trunk-routing

Use the **prefer trunk-routing** command to add a trunk to a list of trunks that are considered first for call routing, regardless of system routing mode or locally configured extensions. Use the **no** form of this command to remove the trunk from the list.

Syntax Description

No subcommands.

Default Values

By default, **prefer trunk-routing** is disabled.

Command History

Release A2	Command was introduced.

Functional Notes

Trunk routing can be specified as a preference for specific trunks, allowing the trunk to be considered first for routing rather than relying on the internal or external nature of the call to dictate whether the trunk or voice station is the first choice routing path. The **prefer trunk-routing** command, executed from a specific trunk's configuration mode, adds the trunk to a list of trunks that are considered first for routing.

By default, no trunk routing preference is set, so that each trunk operates as dictated by normal call routing modes. Adding the trunk routing preference only affects how inbound calls from the specific trunk are handled.

Usage Examples

The following example specifies that trunk routing is preferred on the trunk **T01**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#prefer trunk-routing**

reject-external

Use the **reject-external** command to blocked outbound (external) call attempts. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables packet loss concealment (PLC) on trunk **T01**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#reject-external**

resource-selection

Use the **resource-selection** command to determine how the switchboard uses outbound call resources contained within a time division multiplexing (TDM) based trunk group. Use the **no** form of this command to disable this feature. Variations of this command include:

resource-selection circular
resource-selection circular ascending
resource-selection circular descending
resource-selection linear
resource-selection linear ascending
resource-selection linear descending

Syntax Description

circular	Performs call load balancing among available DS0s/B-channels in this trunk. Subsequent calls will be delivered to the next available DS0/B-channel in a round-robin fashion.
linear	Specifies that a call being delivered to this trunk will be accepted out the first available DS0/B-channel available at the time the call is received.
ascending	Optional. Distributes calls in an order from the lowest to the highest channel (DS0 1, 2, 3 through 24).
descending	Optional. Distributes calls in an order from the highest to the lowest channel (DS0 24, 23, 22 through 1).

Default Values

By default, resource selection is set to **linear**.

Command History

Release 9.3	Command was introduced.
Release 13.1	Command was expanded to include the **ascending** and **descending** subcommands.

Usage Examples

The following example specifies **circular** resource selection:

(config)**#voice trunk t01 type isdn**
(config-t01)**#resource-selection circular**

rtp delay-mode

Use the **rtp delay-mode** command to configure the Realtime Transport Protocol (RTP) jitter buffer packet delay mode settings. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Use the **no** form of this command to return to the default setting. Variations of this command include:

rtp delay-mode adaptive
rtp delay-mode fixed

Syntax Description

adaptive	Configures RTP jitter buffer packet delay to adjust during a call based on network conditions.
fixed	Configures the RTP jitter buffer packet delay to remain constant.

Default Values

By default, this command is set to **adaptive**.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures RTP delay mode as **fixed**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#rtp delay-mode fixed**

rtp dtmf-relay

Use the **rtp dtmf-relay** command to configure the method by which Realtime Transport Protocol (RTP) dual tone multi-frequency (DTMF) events are relayed, either inband in the RTP stream or out-of-band (OOB) using named telephone events (NTEs). RTP DTMF relay is used to prevent the tone (dialed digits) from being corrupted. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp dtmf-relay inband
rtp dtmf-relay nte <*value*>

Syntax Description

inband	Configures RTP DTMF relay events for **inband**.
nte <*value*>	Configures RTP DTMF relay events for NTE. Enter a value between **96** and **127**.

Default Values

By default, the **rtp dtmf-relay** is set for **NTE 101**.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the integrated services digital network (ISDN) trunk.

Usage Examples

The following example configures RTP DTMF relay events for **NTE** with an event value of **101**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#rtp dtmf-relay nte 101**

rtp frame-packetization <*value*>

Use the **rtp frame-packetization** command to configure the Realtime Transport Protocol (RTP) frame packetization time in milliseconds for individual trunks and users. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP frame packetization time value in milliseconds. Select from **10**, **20**, **30**, or **40** milliseconds.

Default Values

By default, the **rtp frame-packetization** time is set to **20** milliseconds on all trunks and users.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the integrated services digital network (ISDN) trunk.
Release R10.8.0	Command was expanded to include **40** milliseconds.

Usage Examples

The following example sets the frame packetization time for trunk **T01** to **20** milliseconds:

(config)**#voice trunk t01 type isdn**
(config-t01)**#rtp frame-packetization 20**

rtp packet-delay

Use the **rtp packet-delay** command to configure the maximum Realtime Transport Protocol (RTP) packet delays. This command is used to set the allowable limits of latency on the network. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp packet-delay fax <*value*>
rtp packet-delay maximum <*value*>
rtp packet-delay nominal <*value*>

Syntax Description

fax <*value*>	Sets the fax delay time in milliseconds. Range is **0** to **500** milliseconds.
maximum <*value*>	Sets the maximum delay time in increments of **10** milliseconds. Range is **40** to **320** milliseconds.
nominal <*value*>	Sets the nominal delay time in increments of **10** milliseconds. Range is **10** to **240** milliseconds.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the RTP fax delay time on trunk **T01** to **10** milliseconds:

(config)**#voice trunk t01 type isdn**
(config-t01)**#rtp packet-delay fax 10**

rtp qos dscp <*value*>

Use the **rtp qos dscp** command to configure the maximum Realtime Transport Protocol (RTP) quality of service (QoS) parameters for differentiated services code point (DSCP).

Syntax Description

<*value*>	Configures the RTP QoS parameter for DSCP. Enter a value between **10** and **63**.

Default Values

By default, no RTP QoS DSCP is configured for this interface.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the integrated services digital network (ISDN) trunk.

Functional Notes

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. QoS is set using a DSCP value. Valid DSCP values are **10** to **63**, and a higher DSCP value has a higher priority. The default DSCP value for RTP is **46**. Remember that if you are using a public IP connection, such as the Internet, for Voice over Internet Protocol (VoIP), end-to-end QoS may not be guaranteed. The default DSCP value for Session Initiation Protocol (SIP) is **26**. To configure QoS for the RTP traffic that carries the voice conversation, use the command **ip rtp qos dscp** followed by the desired DSCP value.

Usage Examples

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. The following example sets the DSCP value for RTP packets that trunk **T02** generates to **60**.

(config)**#voice trunk t02 type isdn**
(config-t02)**#rtp qos dscp 60**

rtp rx-gain *<value>*

Use the **rtp rx-gain** command to specify the Realtime Transport Protocol (RTP) receive (RX) gain or attenuation. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Using the **no** form of this command returns the RTP RX gain or attenuation to the default value.

Syntax Description

<value>	Specifies the RTP RX gain or attenuation in the RTP to time division multiplexing (TDM) direction. Range is **6** to **-14**. Negative values specify attenuation. Positive values specify gain in decibels (dB).

Default Values

By default, RTP RX gain is set to **0** dB.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example specifies the RTP RX gain for integrated services digital network (ISDN) trunk **T01** is **4** dB:

(config)**#voice trunk t01 type isdn**
(config-t01)**#rtp rx-gain 4**

rtp tx-gain <*value*>

Use the **rtp tx-gain** command to specify the Realtime Transport Protocol (RTP) transmit (TX) gain or attentuation. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Using the **no** form of this command returns the RTP TX gain or attenuation to the default value.

Syntax Description

<*value*>	Specifies the RTP TX gain or attenuation in the time division multiplexing (TDM) to RTP direction. Range is **6** to **-14**. Negative values specify attenuation. Positive values specify gain in decibels (dB).

Default Values

By default, RTP TX gain is set to **0** dB.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example specifies the RTP TX gain for integrated services digital network (ISDN) trunk **T01** is **4** dB:

(config)**#voice trunk t01 type isdn**
(config-t01)**#rtp tx-gain 4**

supplementary-service trunk *<trunk id>*

Use the **supplementary-service trunk** command to configure a Session Initiation Protocol (SIP) trunk to provide supplementary services to the integrated services digital network (ISDN) trunk. Use the **no** form of this command to remove the SIP trunk.

Syntax Description

<trunk id>	Specifies a specific voice trunk using the trunk's two-digit identifier following T (for example, T01).

Default Values

By default, there are no trunks configured for supplementary services.

Command History

Release R10.5.0	Command was introduced.

Usage Examples

The following example configures trunk **T01** to be a SIP trunk that provides supplementary services to the ISDN trunk:

(config)**#voice trunk t01 type isdn**
(config-t01)**#supplementary-service trunk T01**

trunk-number <*number*>

Use the **trunk-number** command to define the call routing when direct inward dialing (DID) is disabled. This feature directs incoming calls to the specified number when DID is not present. This command also allows users to activate different system modes of operation that redirect incoming calls to a different number depending on the specified mode. Use the **no** form of this command to disable this feature. Variations of this command include:

trunk-number <*number*>
trunk-number no-number
trunk-number <*system mode*> <*number*>
trunk-number <*system mode*> **no-number**
trunk-number override <*number*>
trunk-number override no-number

Syntax Description

<*number*>	Specifies the number used for call routing when DID is disabled.
<*system mode*>	Optional. Specifies the system mode to configure. Choose from **custom1**, **custom2**, **custom3**, **lunch**, **night**, or **weekend**. Refer to the command *voice system-mode on page 1971* for more information on system modes.
no-number	Specifies no inbound calls are allowed on this trunk.
override	Ignores the programmed system mode schedule.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the feature group D (FGD) trunk options.
Release A1	Command was expanded to include the new subcommands.

Usage Examples

The following example defines call routing on trunk **T02**:

(config)**#voice trunk t02 type isdn**
(config-t02)**#trunk-number 4000**

t38

Use the **t38** command to enable T.38 fax operation. Use the **no** form of this command to disable this feature.

> *The command modem-passthrough on page 5024 must be enabled for T.38 operation to work.*

Syntax Description

No subcommands.

Default Values

By default, T.38 is disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables T.38:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38**

Technology Review

T.38 is an International Telecommunication Union (ITU) specification that allows Group-3 Fax (T.30) data to be transported over the Internet. It is similar to dual tone multi-frequency (DTMF) relay (RFC 2833) in that the digital signal processor (DSP) decodes tones and demodulated fax data and converts them into packets. A similar device on the other end takes the packets/tones and remodulates them so that an analog fax machine on the other end can receive the fax. AOS's previous support (revisions 12 through 15) for fax/modem signals was simply detecting a tone and forcing the coder-decoder (CODEC) into G.711 and disabling/enabling echo cancellers based on the tones detected. When packet loss becomes high, sending faxes over G.711 becomes problematic, due to dropped messages and timeouts/retrains.

T.38 can be used in conjunction with various call-control schemes, such as H.323, Session Initiation Protocol (SIP), and Media Gateway Control Protocol (MGCP). AOS only supports SIP as the call-control method. This is typically referred to T.38/Annex-D. Annex-D describes the Session Initiation Protocol/Session Description Protocol (SIP/SDP) call establishment procedures.

t38 ced auto-generate

Use the **t38 ced auto-generate** command to specify when the digital signal processor (DSP) should regenerate the called station identifier (CED) signal toward the time division multiplexed (TDM) endpoint. If auto-generate is enabled, the DSP generates the CED signal only when it does not receive CED indicator packets from the Voice over IP (VoIP) endpoint. If auto-generate is disabled, the DSP generates the CED signal only when it does receive CED indicator packets from the VoIP endpoint. Using the **no** version of this command disables CED auto-generate.

Syntax Description

No subcommands.

Default Values

By default, CED auto-generate is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example enables CED auto-generate for the T.38 session on the trunk:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 ced auto-generate**

t38 ced length <*time*>

Use the **t38 ced length** command to set the maximum duration of a regenerated called station identifier (CED) signal, in milliseconds, from the digital signal processor (DSP) toward the time division multiplexed (TDM) endpoint when a T.38 session is active. Using the **no** form of this command returns the duration to the default value.

Syntax Description

<*time*>	Specifies the maximum duration of a regenerated CED signal in milliseconds. Valid range is **0** to **4000** ms.

Default Values

By default, the maximum duration of a regenerated CED signal is **3000** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Setting the maximum duration of a regenerated CED signal to **0** effectively prevents any CED generation.

Usage Examples

The following example decreases the maximum duration of the CED signal to **2000** ms for the T.38 session:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 ced length 2000**

t38 cng-relay-selective

Use the **t38 cng-relay-selective** command to enable fax calling tones (CNG) relay only when V.21 messages are not being transmitted. Use the **no** version of this command to disable selective CNG relay.

Syntax Description

No subcommands.

Default Values

Selective CNG relay is disabled by default.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables T.38 CNG relay:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 cng-relay-selective**

t38 ecm

Use the **t38 ecm** command to enable or disable error correction mode (ECM) during T.38 sessions. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 ecm enable
t38 ecm disable

Syntax Description

enable	Enables ECM during T.38 sessions.
disable	Disables ECM during T.38 sessions.

Default Values

By default, ECM is enabled.

Command History

Release R10.8.0	The command was introduced

Usage Examples

The following example disables ECM for T.38 sessions on trunk T01:

((config)**#voice trunk t02 type isdn**
(config-t02)**#t38 ecm disable**

t38 error-correction

Use the **t38 error-correction** command to specify the type of fax error correction. Use the **no** form of this command to disable this feature. Variations of this command include:

t38 error-correction fec
t38 error-correction redundancy

Syntax Description

fec	Specifies forward error correction (FEC) as the fax error correction. FEC is a system of error control where the sender adds redundant data to its messages, allowing the receiver to detect and correct errors (within certain bounds) without the need to request additional data from the sender.
redundancy	Specifies redundancy as the fax error correction. Redundancy error correction replicates the payload a user-specified number of times to determine if errors are present. The number of redundant packets is set using the command *t38 redundancy on page 5049*).

Default Values

By default, **t38 error-correction** is set to **redundancy** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, the NetVanta 6240/6250 Serires, and the NetVanta 640 Series.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default value changed to **fec** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, and the NetVanta 7000 Series products.
Release R10.8.0	The default values for this command were updated.

Usage Examples

The following example sets the **t38 error-correction** to **fec**:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 error-correction fec**

t38 fallback-mode g711

Use the **t38 fallback-mode** command to specify the transmission mode used when T.38 fax relay cannot be successfully negotiated at the time of the fax transfer. Use the **no** form of this command to disable this feature.

Syntax Description

g711	Specifies that fax operation revert back to analog mode (G.711).

Default Values

By default, **t38 fallback-mode** is to **G.711**.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **G.711**.

Usage Examples

The following example enables the **t38 fallback-mode** on trunk **T02**:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 fallback-mode g711**

t38 generate-cng

Use the **t38 generate-cng** command to specify whether the digital signal processor (DSP) will begin a T.38 session by generating the calling signal (CNG) toward the time division multiplexed (TDM) endpoint. Using the **no** version of this command disables CNG generation.

Syntax Description

No subcommands.

Default Values

By default, CNG generation is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

With the introduction of this command, the CNG generation behavior of the T.38 session is now configurable. In AOS firmware prior to A5.01, this behavior was not configurable, but rather was set to always generate this signal.

Usage Examples

The following example enables CNG generation for the T.38 session:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 generate-cng**

t38 max-buffer <*value*>

Use the **t38 max-buffer** command to set the maximum buffer size for T.38 fax operation. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-buffer** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **800** bytes.

Default Values

By default, the maximum buffer size is set to **200**.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-buffer** to **100**:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 max-buffer 100**

t38 max-datagram <*value*>

Use the **t38 max-datagram** command to set the maximum datagram value in this unit. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-datagram** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **300** bytes.

Default Values

By default, the maximum datagram value is set to **72** bytes.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **72** bytes.

Usage Examples

The following example sets the **t38 max-datagram** to **100**:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 max-datagram 100**

t38 max-rate

Use the **t38 max-rate** command to specify the fax maximum rate. The actual transmission rate could be lower than specified rate if the receiving end cannot support the maximum rate. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 max-rate 14400
t38 max-rate 12000
t38 max-rate 2400
t38 max-rate 4800
t38 max-rate 7200
t38 max-rate 9600

Syntax Description

14400	Specifies 14400 bits per second (bps) as fax maximum rate.
12000	Specifies 12000 bps as fax maximum rate.
2400	Specifies 2400 bps as fax maximum rate.
4800	Specifies 4800 bps as fax maximum rate.
7200	Specifies 7200 bps as fax maximum rate.
9600	Specifies 9600 bps as fax maximum rate.

Default Values

By default, the maximum fax rate is set to **14400** bps.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-rate** to **4800** bps:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 max-rate 4800**

t38 redundancy

Use the **t38 redundancy** command to set the number of redundant packets sent when the **t38 error-correction redundancy** feature is enabled. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 redundancy high-speed <*value*>
t38 redundancy low-speed <*value*>

Syntax Description

high-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for data messages (high-speed fax machine image data). Range is **0** (no redundancy) to **4** packets.
low-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for the signaling messages (low-speed fax machine protocol). Range is **0** (no redundancy) to **7** packets.

Default Values

By default, high-speed and low-speed redundancy values are set to **0** (no redundancy).

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables **t38 error-correction redundancy** and sets the number of redundant data messages to **3**:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 error-correction redundancy**
(config-t02)**#t38 redundancy high-speed 3**

t38 v21-preamble-timeout *<value>*

Use the **t38 v21-preamble-timeout** command to set the maximum amount of time that the digital signal processor (DSP) waits for peer device activity after starting to transmit a V.21 preamble event before spoofing a response to the time division multiplexed (TDM) endpoint. Using the **no** version of this command returns the timeout value to the default setting.

Syntax Description

<value>	The time, in milliseconds, that the DSP will wait for peer activity. Valid range is **1** to **3000** ms.

Default Values

By default, the V.21 preamble timeout is set to **1700** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example specifies the V.21 preamble timeout value as **2000** ms:

(config)**#voice trunk t02 type isdn**
(config-t02)**#t38 v21-preamble-timeout 2000**

vad

Use the **vad** command to enable voice activity detection (VAD). VAD blocks out noise categorized as silence during a voice connection. The silent voice packets are not transmitted, allowing bandwidth usage to be reduced. Although VAD saves bandwidth, the quality of the voice call may be compromised. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, VAD is enabled for all T1 robbed-bit signaling RBS trunks and users.

Command History

Release 9.3	Command was introduced.
Release 11.1	Command was expanded to include the integrated services digital network (ISDN) trunk.

Usage Examples

The following example enables voice activation detection on trunk **T01**:

(config)**#voice trunk t01 type isdn**
(config-t01)**#vad**

VOICE SIP TRUNK COMMAND SET

Session Initiation Protocol (SIP) trunking is a packet-based voice service that routes calls over an IP network to an IP-compatible private branch exchange (PBX) or voice switch using SIP signaling to place and receive calls. The typical SIP trunk service provider offers extensive cost savings, compared to conventional trunk services. The IP connection to the provider carries all traffic, such as local, long distance, and toll free calls, video, email, Internet, data, and other media over a single circuit. Calls into public switched telephone networks (PSTNs) are also handled by the SIP service provider by passing the calls off to a media gateway that connects to the PSTN for users not using Voice over Internet Protocol (VoIP) service.

SIP trunks are configured over data connections. Thus, they can be configured over an Ethernet connection or a T1 connection.

To create a SIP trunk and enter the Voice SIP Trunk Configuration mode, enter the **voice trunk type sip** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type sip
(config-t01)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

alc on page 5055
alert-info on page 5056
authentication username <username> password <password> on page 5057
busy all on page 5058
busy-out monitor track <name> on page 5059
caller-id-override on page 5060
check-supported replaces on page 5062
codec-list <name> on page 5063
conferencing-uri <value> on page 5065
default-ring-cadence on page 5066
dial-string source on page 5067

alc

Use the **alc** command to enable automatic level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature. Variations of this command include:

alc
alc level -16
alc level -17
alc level -18
alc level -19
alc level -20
alc level -21
alc level -22

Syntax Description

level -16	Optional. Specifies the ALC attenuation level is -16 dBm0.
level -17	Optional. Specifies the ALC attenuation level is -17 dBm0.
level -18	Optional. Specifies the ALC attenuation level is -18 dBm0.
level -19	Optional. Specifies the ALC attenuation level is -19 dBm0.
level -20	Optional. Specifies the ALC attenuation level is -20 dBm0.
level -21	Optional. Specifies the ALC attenuation level is -21 dBm0.
level -22	Optional. Specifies the ALC attenuation level is -22 dBm0.

Default Values

By default, ALC is disabled.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.
Release A2.04	Command was expanded to include the **level** parameters.

Usage Examples

The following example activates the ALC on trunk **T01**:

(config)**#voice trunk t01 type sip**
(config-t01)**#alc**

alert-info

Use the **alert-info** command to allow the alert information attribute on incoming and/or outgoing auto answer alert information. Use the **no** form of this command to cancel the setting. Variations of this command include:

alert-info incoming auto-answer
alert-info outgoing auto-answer

Syntax Description

incoming auto-answer	Specifies processing incoming ALERT-INFO attribute.
outgoing auto-answer	Specifies allowing the outgoing ALERT-INFO auto-answer attribute.

Default Values

By default, both incoming and outgoing auto answer alert information is allowed on the NetVanta 7000 Series in the ALERT-INFO messages. However, both are disabled by default in the IP business gateways (IPBGs). The IPBGs will ignore incoming auto answer in the ALERT-INFO messages, and will not send the information on outgoing trunks.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example blocks outgoing alert-info auto-answer attribute on trunk **T01**:

(config)**#voice trunk t01 type sip**
(config-t01)**#alert-info outgoing auto-answer**

authentication username <*username*> password <*password*>

Use the **authentication username password** command to enable authentication security between the Session Initiation Protocol (SIP) server and the unit. Each port that registers with the SIP server will use the defined **username** and **password**. Use the **no** form of this command to return to the default setting.

Syntax Description

username <*username*>	Specifies a string to be sent as the user name in authentication.
password <*password*>	Specifies a string to be sent as the password in authentication.

Default Values

By default, authentication is not enabled.

Command History

Release 9.3	Command was introduced.

Functional Notes

If all users on the trunk use the same user name/password, enter the user name and password for authentication under the trunk. Otherwise, enter authentication information for each user individually in the Voice User command set that overrides the setting of this command. Refer to *Voice User Account Command Set on page 4564* for more information.

Usage Examples

The following example configures a user name of **iaduser** and password of **totalaccess** at the trunk level:

(config)**#voice trunk t01 type sip**
(config-t01)**#authentication username iaduser password totalaccess**

busy all

Use the **busy all** command to set all level zero digital signals (DS0s) to busy so that no calls are allowed inbound or outbound. If any calls are active at the time this command is issued, the calls will stay active until either party terminates the call. Once terminated, the DS0s are busied out. Use the **no** form of this command to disable this feature. Variations of this command include:

busy all
busy all now

Syntax Description

now	Optional. Immediately terminates calls that are active at the time the command is issued.

Default Values

By default, this command is disabled.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was added to the Voice Trunk Session Initiation Protocol (SIP) command set.

Usage Examples

The following example sets all DS0s on trunk **T01** to busy and terminates calls that are active at the time the command is issued:

(config)**#voice trunk t01 type sip**
(config-t01)**#busy all now**

busy-out monitor track <*name*>

Use the **busy-out monitor track** command to automatically take a voice trunk out of service based on one or more conditions. The primary application of this feature is to signal to an attached private branch exchange (PBX) that because calls routed to the integrated access device (IAD) could fail due to loss of Session Initiation Protocoal (SIP) trunk connectivity, it should attempt to route the call via another interface. For more information on creating tracks, refer to *track <name> on page 1886* and the *Network Monitor Track Command Set on page 4098*. Use the no form of this command to remove a track from busy-out monitoring.

Syntax Description

<name>	Specifies the name of the track to monitor.

Default Values

No default values are necessary for this command.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example shuts down trunk **T01** when the **on_fail** track fails:

(config)**#voice trunk t01 type sip**
(config-t01)**#busy-out monitor track on_fail**

caller-id-override

Use the **caller-id-override** command to replace the calling party information for this trunk with a specific number. This command is used to conceal a user's name and number or to display a different name and number for internal or external caller ID. Use the **no** form of this command to cancel the setting. Variations of this command include:

caller-id-override emergency-outbound <*number*>
caller-id-override emergency-outbound match-substitute
caller-id-override name-inbound <*name*>
caller-id-override name-inbound <*name*> **if-unavailable**
caller-id-override number-inbound <*number*>
caller-id-override number-inbound <*number*> **if-no-cpn**
caller-id-override number-inbound <*number*> <*trunk id*>
caller-id-override privacy-outbound match-substitute

Syntax Description

emergency-outbound	Replaces the calling party number for outbound emergency calls.
<*number*>	Specifies the number to replace the calling party number for outbound emergency calls.
match-substitute	Specifies that the configured automatic number identification (ANI) match substitution is used for outbound emergency calls.
name-inbound <*name*>	Specifies the name to replace the calling party name for inbound calls.
if-unavailable	Specifies that the calling party name is replaced only if the calling party name is unavailable.
number-inbound <*number*>	Specifies the number to replace the calling party number for inbound calls.
<*trunk id*>	Optional. Specifies the trunk ID (**Txx**) for outbound calls.
if-no-cpn	Optional. Specifies that the calling party number is replaced only if the calling party number is unavailable.
privacy-outbound	Replaces the calling party number on anonymous outbound calls.
match-substitute	Specifies that the configured ANI match substitution is used for anonymous outbound calls.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 15.1	Command was expanded.
Release 16.1	Command was expanded to include the **if-no-cpn** parameter.
Release A4.01	Command was expanded to include the **match-substitute** parameter.
Release R11.8.0	Command was expanded to include the **privacy-outbound** parameter.

Usage Examples

The following example sets the caller ID override number on the trunk where the command is issued:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#caller-id-override number-inbound 555-8000**

check-supported replaces

Use the **check-supported replaces** command to check all support extensions on outbound messages and only send replaces when supported by the far-end device. Otherwise, replaces are automatically sent regardless of the far-end capabilities. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets all DS0s on trunk **T01** to busy and terminates calls that are active at the time the command is issued:

(config)**#voice trunk t01 type sip**
(config-t01)**#check-supported replaces**

codec-list *<name>*

Use the **codec-list** command to specify the coder-decoder (CODEC) list to be used by this account. This CODEC can be used for normal voice traffic or for Session Border Controller (SBC) transcoding. Use the **no** form of this command to remove the CODEC list from the account. Variations of this command include:

codec-list *<name>*
codec-list *<name>* **both**
codec-list *<name>* **in**
codec-list *<name>* **out**
codec-list any
codec-list any both
codec-list any in
codec-list any out

Syntax Description

<name>	Specifies the CODEC list to be used for this account.
any	Specifies that any possible CODEC is allowed on this account.
both	Optional. Specifies that the CODEC list is applied to both transmitted and received Session Description Protocol (SDP) transmissions.
in	Optional. Specifies that the CODEC list is applied to received SDP only.
out	Optional. Specifies that the CODEC list is applied to transmitted SDP only.

Default Values

By default, no CODEC lists are assigned.

Command History

Release R10.4.0	Command was introduced and replaced the **codec-group** command.

Functional Notes

The **codec-list** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893***.**

In addition, CODEC lists can be used for the SBC transcoding feature. For more information about this feature, its uses, and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

> NOTE *Because you can choose to specify that any CODEC is used by a Session Initiation Protocol (SIP) endpoint with the **any** keyword, do not create a CODEC list with the name of **any**.*

Usage Examples

The following example applies the CODEC list **LIST1** to incoming SDP traffic on trunk **T01**:

(config)**#voice trunk t01 type sip**
(config-t01)**#codec-list LIST1 in**

conferencing-uri *<value>*

Use the **conferencing-uri** command to configure a conference application server uniform resource identifier (URI) that controls and uniquely identifies a conference. Use the **no** form of this command to return to the default setting.

Syntax Description

<value>	Specifies the extension or complete URI of the conference application server.

Default Values

By default, **conferencing-uri** is not configured.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the **conferencing-uri** to **0606**:

(config)**#voice trunk t01 type sip**
(config-t01)**#conferencing-uri 0606**

default-ring-cadence

Use the **default-ring-cadence** to set the default ring cadence for incoming Session Initiation Protocol (SIP) calls that do not contain an Alert-Info header preference. Use the **no** form of this command to return to the default setting. Variations of this command include:

default-ring-cadence external
default-ring-cadence internal

Syntax Description

external	Sets the default ring cadence for incoming calls to external.
internal	Sets the default ring cadence for incoming calls to internal.

Default Values

By default, the inbound ring cadence is set to external.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example sets the **default-ring-cadence** to **internal**:

(config)**#voice trunk t01 type sip**
(config-t01)**#default-ring-cadence internal**

dial-string source

Use the **dial-string source** command to set the Session Initiation Protocol (SIP) dialing string field of your choice. Use the **no** form of this command to remove the specified setting. Variations of this command include the following:

dial-string source request-uri
dial-string source to

Syntax Description

request-uri	Specifies the Request URI user field as the dialing string source.
to	Specifies the To header field as the dialing string source.

Default Values

No default values are necessary for this command.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example enables the To header user field as the **dial-string** for this trunk:

(config)**#voice trunk t01 type sip**
(config-t01)**#dial-string source to**

diversion-supported

Use the **diversion-supported** command to apply a Session Initiation Protocol (SIP) Diversion header to redirected calls on the trunk. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled on the NetVanta 7000 Series products. By default, this feature is enabled on the Total Access 900(e) Series products and NetVanta 6000 Series products.

Command History

Release A2.03	Command was introduced.

Functional Notes

This feature retains the originating number when a call is processed through an auto attendant, transferred from a user extension, or is forwarded by a user phone to an external number. For these calls, the number included in the From field of the SIP messages are subject to the automatic number identification (ANI) substitution and a SIP Diversion header is added with the original caller ID number. Calls from internal extensions are subject to the ANI substitution configured on the trunk without the addition of a SIP Diversion header.

Usage Examples

The following example enables **diversion-supported**:

(config)**#voice trunk t01 type sip**
(config-t01)**#diversion-supported**

domain *<name>*

Use the **domain** command to configure the assigned domain name for host messages. The domain is an unique identifier for the Session Initiation Protocol (SIP) users on the trunk. Use the **no** form of this command to disable this feature.

Syntax Description

<name>	Specifies the domain name for the SIP trunk commands.

Default Values

By default, no domain is configured.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the domain name as **home.com**:

(config)**#voice trunk t01 type sip**
(config-t01)**#domain home.com**

grammar alert-info url <*url*>

Use the **grammar alert-info url** command to specify the Alert-Info header construction for Session Initiation Protocol (SIP) trunk messages. Use the **no** form of this command to return to the default setting.

Syntax Description

<*url*>	Specifies the Alert-Info Hypertext Transfer Protocol (HTTP) universal resource locator (URL) header format.

Default Values

By default, the local loopback address is the host in the Alert-Info header (**127.0.0.1**).

Command History

Release A2	Command was introduced.

Usage Examples

The following example sets the Alert-Info header to use a specific URL as shown in the sample header below:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar alert-info url www.notused.com**

Sample header:

Alert-Info:<http://www.notused.com>;info=alert-internal

grammar contact host local

Use the **grammar contact host local** command to configure the Contact header on Session Initiation Protocol (SIP) messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip grammar contact host local
sip grammar contact host local fqdn

Syntax Description

host local	Specifies that the local IP is used in the SIP Contact header.
fqdn	Optional. Specifies that a fully qualified domain name (FQDN) is used in the SIP Contact header.

Default Values

By default, SIP Contact headers use a local IP.

Command History

Release R13.11.0	Command was introduced.

Usage Examples

The following example sets the Contact header format to use an FQDN:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar contact host local fqdn**

grammar contact host port persistent

Use the **grammar contact host port persistent** command to configure the AOS device to use the Transmission Control Protocol (TCP) port from which AOS initiated a Transport Layer Security (TLS) connection in the Contact uniform resource identifier (URI) sent by AOS. Use the **no** form of this command to disable this feature.

Syntax Description

host	Specifies the Contact header Host field setting.
port	Specifies the Contact header host port.
persistent	Specifies that the persistent connection port should be used for the Contact header host port.

Default Values

No default values are necessary for this command.

Command History

Release R11.5.0	Command was introduced

Functional Notes

This configuration is useful when using client-only authentication. With this type of authentication, a persistent connection is established to the SIP server. Many SIP servers and enterprise session border controllers (eSBCs) need to see the TCP port from which AOS initiated the TLS connection in the Contact URI sent by AOS.

Usage Examples

The following example specifies that AOS device should use the TCP port from which AOS initiated the TLS connection in the Contact URI sent by AOS:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar contact host port persistent**

grammar from

Use the **grammar from** command to configure the From header on Session Initiation Protocol (SIP) messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar from host domain
grammar from host local
grammar from host local fqdn
grammar from host override registered-users domain
grammar from host override registered-users local
grammar from host override registered-users sip-server
grammar from host sip-server
grammar from user domestic
grammar from user domestic <*Txx*>
grammar from user international
grammar from user international <*Txx*>

Syntax Description

host	Specifies the Host field formatting for the From header.
domain	Specifies the trunk domain setting for formatting the From header.
local	Specifies the local IP address for formatting the From header.
fqdn	Optional. Specifies a fully qualified domain name (FQDN) is used for formatting the From header.
override registered-users	Overrides the current **grammar from host** setting for SIP messages originating from registered users.
sip-server	Specifies the SIP server settings for formatting the From header.
user	Specifies the User field formatting for the From header.
domestic	Specifies domestic formatting for the From user header.
international	Specifies international formatting for the From user header.
<*Txx*>	Optional. Indicates a two-digit trunk identifier (for example, **T01**).

Default Values

By default, the host for formatting messages is **sip-server**, and the default for the user format is **domestic**.

Command History

Release A2	Command was introduced.
Release A5.01	Command was expanded to include the **override registered-users** parameter.
Release R10.1.0	Command was introduced.
Release R13.11.0	Command was expanded to include the **fqdn** parameter.

Functional Notes

Omitting the trunk identifier when issuing the **grammar from user** command specifies the User header globally.

Usage Examples

The following example sets the From header format to use an FQDN:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar from host local fqdn**

The following example sets the From header format to use calling party format on trunk **T02**:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar from user domestic T02**

Technology Review

This technology review provides information about the E.164 recommendation for international numbering plans and telephone number formats.

A fully specified telephone number can have a maximum of 15 digits, including country code, area code, and the subscriber's number. These numbers usually consist of a + prefix. E.164 numbers exclude dialing prefixes. The most familiar prefixes are international direct dialing (IDD) and national direct dialing (NDD). In countries other than the United States, the IDD and NDD are represented by different numbers.

Additionally, E.123 describes the use of + to indicate a fully specified international number. The + is used in SIP headers to provide consistency across national and international phone calls.

AOS products provide support for E.164 by being able to specify a country code and an IDD prefix. Nationally formatted telephone numbers are converted to international format by prefixing them with + and the country code. On outbound international calls, + is substituted for the IDD. On incoming international calls, the + is removed. If the country code matches the configured value, it too is removed.

*Setting the From header to **international** will cause phone numbers to be formatted as indicated by E.164. The country code must be configured, and the number must be of type **national** for this feature to work successfully.*

grammar p-asserted-identity host

Use the **grammar p-asserted-identity host** command to configure the P-Asserted Identity header host format for the Session Initiation Protocol (SIP) trunk. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar p-asserted-identity host domain
grammar p-asserted-identity host local
grammar p-asserted-identity host local fqdn
grammar p-asserted-identity host sip-server

Syntax Description

domain	Specifies the domain host for formatting the header.
local	Specifies the local IP as host for formatting the header.
fqdn	Optional. Specifies that a fully qualified domain name (FQDN) is used for formatting the header.
sip-server	Specifies the SIP server as host for formatting the header.

Default Values

By default, the host for formatting messages is **sip-server**.

Command History

Release A2	Command was introduced.
Release R13.11.0	Command was expanded to include the **fqdn** parameter.

Usage Examples

The following example sets the p-asserted-identity header host format to use an FQDN for constructing the header:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar p-asserted-identity host local fqdn**

grammar p-early-media supported

Use the **grammar p-early-media supported** command to enable sending a P-Early-Media header with a value of "supported" in INVITE, PRACK, and UPDATE requests sent on the Session Initiation Protocol (SIP) trunk. Use the **no** form of this command to disable support for the early media detection feature.

Syntax Description

No subcommands.

Default Values

By default, sending of the P-Early-Media header is disabled.

Command History

Release 13.6.0	Command was introduced.

Functional Notes

Support for sending the P-Early-Media header can be configured on a per-trunk basis, using the **grammar p-early-media supported** command as described here, or it can be configured globally, using the command *sip grammar p-early-media supported on page 1715*. The trunk setting will always take precedence over the globally configured setting.

Usage Examples

The following example configures a trusted domain on the trunk and enables sending the P-Early-Media header:

(config)**#voice trunk t01 type sip**
(config-t01)**#trust-domain**
(config-t01)**#grammar p-early-media supported**

grammar proxy-require privacy

Use the **grammar proxy-require privacy** command to add privacy to Proxy-Require header format for Session Initiation Protocol (SIP) trunk. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release A2	Command was introduced.

Usage Examples

The following example allows a Proxy-Require header to be added to packets containing a privacy header:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar proxy-require privacy**

grammar refer-to

Use the **grammar refer-to** command to configure the Session Initiation Protocol (SIP) Refer-To header on intratrunk attended transfers. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar refer-to intratrunk-attended-transfer source contact
grammar refer-to intratrunk-attended-transfer source to-from

Syntax Description

intratrunk-attended-transfer source	Specifies the source for Refer-To header of an intratrunk attended transfer.
contact	Specifies the Contact header as the source for the Refer-To header.
to-from	Specifies either the To or From header as the source for Refer-To header.

Default Values

By default, the To or From header is the source for the Refer-To header on intratrunk attended transfers.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example specifies the Contact header as the source for the Refer-To header of an intratrunk attended transfer:

(config)**#voice trunk t01 type sip**
(config-T01)**#grammar refer-to intratrunk-attended-transfer source contact**

grammar request-uri

Use the **grammar request-uri** command to format the Request uniform resource identifier (URI) for Session Initiation Protocol (SIP) trunk messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar request-uri host domain
grammar request-uri host sip-server
grammar request-uri host-resolve
grammar request-uri transmit-network-selection <*parameter name*>

Syntax Description

host domain	Specifies the trunk domain setting for formatting the Request-URI header.
host sip-server	Specifies the trunk SIP server setting for formatting the Request-URI header.
host-resolve	Enables the local unit to resolve the domain before constructing the Request-URI header.
transmit-network-selection <*parameter name*>	Specifies that Transmit Network Selection is included in the Request URI.

Default Values

By default, the host for formatting messages is **sip server**, and **host-resolve** is disabled.

Command History

Release A2	Command was introduced.
Release R10.1.0	Command was added to the VQM Reporter command set.
Release R13.8.0	Command was expanded to include the **transmit-network-selection** parameter.

Usage Examples

The following example enables SIP trunk messages to resolve the Request URI from the host domain:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar request-uri host domain**

The following example enables SIP trunk messages to resolve the Request URI from the local unit:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar request-uri host-resolve**

grammar require 100rel

Use the **grammar require 100rel** command to add **100rel** to the Require header format. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, **grammar require 100rel** is disabled.

Command History

Release A2	Command was introduced.

Functional Notes

This command enables or disables the sending of reliable provisional responses to clients that *support* 100rel. Reliable provisional responses will always be sent to clients that *require* 100rel even with **grammar require 100rel** disabled.

Usage Examples

The following example enables **grammar require 100rel**:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar require 100rel**

Technology Review

There are two Require headers that may use the 100rel tag, one in the initial request, and one in the provisional response.

The user agent client (UAC) is used to initiate Session Initiation Protocol (SIP) requests. When the UAC creates a new request, it can require reliable provisional responses for that request by adding the option tag 100rel to the Require header of that request.

The user agent server (UAS) contacts the user when SIP requests are received, and returns responses on behalf of the user, using provisional responses for request progress information. Provisional responses (100 to 199) are transmitted on a best-effort basis. By using reliable provisional responses, responses are sent by the UAS until they are acknowledged as received. This is especially beneficial when sending provisional responses over an unreliable transport, such as User Datagram Protocol (UDP).

The UAS must send any non-100rel provisional responses reliably if the initial request contained a Require header field with the option tag 100rel. If the UAS is unwilling to do so, it must reject the initial request with a Bad Extension message and include an Unsupported header field containing the option tag 100rel. If the client *supports* 100rel, the UAS has the *option* of sending provisional responses with or without the Require 100rel tag as instructed by the **grammar require 100rel** command.

grammar supported 100rel

Use the **grammar supported 100rel** command to include 100rel in the supported header of the Session Initiation Protocol (SIP) trunk message. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, **grammar supported 100rel** is disabled.

Command History

Release A2	Command was introduced.

Usage Examples

The following example enables **grammar supported 100rel**:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar supported 100rel**

grammar to

Use the **grammar to** command to configure the To header host format of Session Initiation Protocol (SIP) trunk messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

grammar to host domain
grammar to host sip-server

Syntax Description

host domain	Specifies using the trunk domain setting to format the To header.
host sip-server	Specifies using the trunk SIP server settings to format the To header.

Default Values

By default, the host for formatting messages is **sip server**.

Command History

Release A2	Command was introduced.
Release R10.1.0	Command was added to the VQM Reporter command set.

Usage Examples

The following example configures the To header format construction to use the trunk domain:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar to host domain**

grammar user-agent

Use the **grammar user-agent** command to configure the user agent (UA) header format in Session Initiation Protocol (SIP) messages for the trunk. The UA header can be given the default value for the product, a user-defined value, or no value at all, in which case the UA header is not sent in SIP messages. In addition, other specific values can be included in the UA header. Use the **no** form of this command to return to the configured system value. Variations of this command include the following:

grammar user-agent <*word*>
grammar user-agent default
grammar user-agent include custom-text <*word*>
grammar user-agent include firmware-version
grammar user-agent include hostname
grammar user-agent include serial-number
grammar user-agent none

Syntax Description

<*word*>	Specifies a word as a user-defined value to replace the default UA value. Maximum 128 letters.
default	Returns the UA header field to the default value.
include	Specifies that additional information is included in the UA header.
custom-text <*word*>	Specifies that a user-defined value is included in the UA header. Maximum 128 letters.
firmware-version	Specifies that the firmware version is included in the UA header.
hostname	Specifies that the host name is included in the UA header.
serial-number	Specifies that the serial number is included in the UA header.
none	Disables the UA header field resulting in no UA header sent in SIP messages.

Default Values

By default, the UA value is set to the system value of the product specified by the Global Configuration mode command *sip grammar user-agent on page 1722*.

Command History

Release R10.3.0	Command was expanded to include the **include** parameters.

Usage Examples

The following example removes the UA header field from SIP messages on the trunk:

(config)**#voice trunk t01 type sip**
(config-t01)**#grammar user-agent none**

hmr

Use the **hmr** command to apply a Session Initiation Protocol (SIP) header manipulation rule (HMR) policy to the SIP traffic on a specific SIP trunk. Use the **no** form of this command to remove the HMR policy. Variations of this command include:

hmr <*name*> **in**
hmr <*name*> **out**

Syntax Description

<*name*>	Specifies the name of the HMR policy to apply to SIP messaging on the trunk.
in	Specifies the HMR policy is applied to inbound SIP messaging received on the trunk.
out	Specifies the HMR policy is applied to outbound SIP messaging transmitted on the trunk.

Default Values

By default, there are no configured HMR options.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

For more information about SIP HMR, its uses and configuration, refer to the configuration guide *Manipulating SIP Headers and Messages in AOS,* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example adds the HMR policy **MYPOLICY1** to the T01 SIP trunk for inbound SIP traffic:

(config)**#voice trunk t01 type sip**
(config-t01)**#hmr MYPOLICY1 in**

incoming-music-on-hold

Use the **incoming-music-on-hold** command to activate music on hold for hold re-invites on Session Initiation Protocol (SIP) trunk calls. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example activates music on hold for hold re-invites on SIP trunk calls:

(config)**#voice trunk t01 type sip**
(config-t01)**#incoming-music-on-hold**

match ani <*template*> add diversion <*template*>

Use the **match ani add diversion** command to add Session Initiation Protocol (SIP) Diversion headers to outgoing SIP messages. Use the **no** form of this command to remove the Diversion header from the SIP message. Variations of this command include:

match ani <*template*> **add diversion** <*template*>
match ani <*template*> **add diversion** <*template*> <*diversion type*> <*screening type*> <*privacy setting*>

Syntax Description

ani <*template*>	Specifies the source automatic number identification (ANI) information to be matched. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
add	Specifies that when the match source matches the match source template, SIP Diversion headers are added to the SIP trunk messages.
diversion <*template*>	Specifies the match target and match target template used to execute the command action when adding SIP Diversion headers to SIP messages. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
<*diversion type*>	Optional. Specifies the reason for the diversion. If you specify the diversion type, you must also specify whether or not the diversion is screened by the network, and whether diversion privacy is used. Diversion reasons include the following:

away	Diverts the message if the receiving SIP agent is away.
deflection	Diverts the message if the receiving SIP agent is deflecting calls.
do-not-disturb	Diverts the message if the receiving SIP agent has do-not-disturb enabled.
follow-me	Diverts the message if the receiving SIP agent has FindMe-FollowMe enabled.
no-answer	Diverts the message if the receiving SIP agent does not answer.
out-of-service	Diverts the message if the receiving SIP agent is out-of-service.
time-of-day	Diverts the message if the message is sent at a particular time of day.
unavailable	Diverts the message if the receiving SIP agent is unavailable.
unconditional	Diverts the message on an unconditional basis.
unknown	Diverts the message if an unknown error occurs.
user-busy	Diverts the message if the receiving SIP agent is busy.

<screening type>	Optional. Specifies whether the diversion is screened by the network. Screening types include:	
	no	Specifies that the diversion used is not screened by the network.
	yes	Specifies that the diversion used is screened by the network.
<privacy setting>	Optional. Specifies whether privacy is used when SIP Diversion headers are added to the SIP messages. Privacy settings include:	
	full	Specifies that the diversion uses full privacy.
	off	Specifies that the diversion does not use privacy.

Default Values

By default, SIP diversions are specified as unconditional (**unconditional**), do not use network screening (**no**), and do not use privacy (**off**).

This command can get very lengthy. To shorten the length of the command, you must elect to use all default values for the diversion options, or you must override all options.

Command History

Release A4.01	Command was introduced.

Functional Notes

Both match source and match target templates are defined in the same way as dial plan entries.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8

6) 1234 Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

In the following example command, the match source template is in **bold**:

match ani **!2565558XXX** add diversion 2565558000 unconditional yes full

*In this example, the template includes a **!** at the beginning. The **!** indicates that the inverse of the template is matched. Inverse matching can only be used with the match source template and requires a static target template (the target template cannot contain wildcards).*

For additional information about configuring SIP Diversion headers in SIP messaging, refer to the quick configuration guide, *Modifying SIP Headers to SIP Trunks in AOS Voice Products* available online at https://supportcommunity.adtran.com.

Usage Examples

In the following example, the SIP trunk (**t01**) is configured so that when the ANI source template (**2565558XXX**) is matched, an unconditional SIP Diversion header with a target template of **2565558000** and network screening and full privacy are added to the message.

(config)**#voice trunk t01**
(config-T01)**#match ani 2565558XXX add diversion 2565558000 unconditional yes full**

match ani <*template*> add p-asserted-identity <*template*>

Use the **match ani add p-asserted-identity** command to add a P-Asserted-Identity header to an outgoing Session Initiation Protocol (SIP) message. Use the **no** form of this command to remove the P-Asserted-Identity header.

Syntax Description

ani <*template*>	Specifies the source ANI information to be matched. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
add	Specifies that when the match source matches the match source template, SIP headers are added to the SIP trunk messages.
p-asserted-identity <*template*>	Specifies that it is a P-Asserted-Identity header that is added to the SIP message and specifies the match target template. Templates are entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.

Default Values

By default, P-Asserted-Identity headers are not added to SIP messages.

Command History

Release A4.01	Command was introduced.

Functional Notes

Both match source and match target templates are defined in the same way as dial plan entries.

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits

5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

In the following example command, the match source template is in **bold**:

match ani **!2565558XXX** add diversion 2565558000 unconditional yes full

*In this example, the template includes a **!** at the beginning. The **!** indicates that the inverse of the template is matched. Inverse matching can only be used with the match source template and requires a static target template (the target template cannot contain wildcards).*

For additional information about configuring SIP Diversion headers in SIP messaging, refer to the quick configuration guide, *Modifying SIP Headers to SIP Trunks in AOS Voice Products* available online at https://supportcommunity.adtran.com.

Usage Examples

In the following example, a P-Asserted-Identity header is adding to a SIP message when the ANI source template of **2565558XXX** is matched with the target template of **2565558000**:

(config)**#voice trunk t01**
(config-T01)**#match ani 2565558XXX add p-asserted-identity 2565558000**

match ani <*template*> replace diversion <*template*>

Use the **match ani replace diversion** command to replace Session Initiation Protocol (SIP) Diversion headers on outgoing SIP messages. Use the **no** form of this command to revert to the original header on the SIP message. Variations of this command include:

match ani <*template*> **replace diversion** <*template*>
match ani <*template*> **replace diversion** <*template*> <*diversion type*> <*screening type*> <*privacy setting*>

Syntax Description

ani <*template*>	Specifies the source automatic number identification (ANI) information to be matched. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
replace	Specifies that when the match source matches the match source template, SIP Diversion headers are replaced on the SIP trunk messages.
diversion <*template*>	Specifies the match target and match target template used to execute the command action when replacing SIP Diversion headers in SIP messages. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
<*diversion type*>	Optional. Specifies the reason for the diversion. If you specify the diversion type, you must also specify whether or not the diversion is screened by the network, and whether diversion privacy is used. Diversion reasons include the following:

away	Diverts the message if the receiving SIP agent is away.
deflection	Diverts the message if the receiving SIP agent is deflecting calls.
do-not-disturb	Diverts the message if the receiving SIP agent has do-not-disturb enabled.
follow-me	Diverts the message if the receiving SIP agent has FindMe-FollowMe enabled.
no-answer	Diverts the message if the receiving SIP agent does not answer.
out-of-service	Diverts the message if the receiving SIP agent is out-of-service.
time-of-day	Diverts the message if the message is sent at a particular time of day.
unavailable	Diverts the message if the receiving SIP agent is unavailable.
unconditional	Diverts the message on an unconditional basis.
unknown	Diverts the message if an unknown error occurs.
user-busy	Diverts the message if the receiving SIP agent is busy.

<screening type>	Optional. Specifies whether the diversion is screened by the network. Screening types include:	
	no	Specifies that the diversion used is not screened by the network.
	yes	Specifies that the diversion used is screened by the network.
<privacy setting>	Optional. Specifies whether privacy is used when SIP Diversion headers are added to the SIP messages. Privacy settings include:	
	full	Specifies that the diversion uses full privacy.
	off	Specifies that the diversion does not use privacy.

Default Values

By default, SIP diversions are specified as unconditional (**unconditional**), do not use network screening (**no**), and do not use privacy (**off**).

This command can get very lengthy. To shorten the length of the command, you must elect to use all default values for the diversion options, or you must override all options.

Command History

Release A4.05	Command was introduced.

Functional Notes

The following are example template entries using wildcards:

Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8

6) 1234 Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

In the following example command, the match source template is in **bold**:

match ani **!2565558XXX** replace diversion 2565558000 unconditional yes full

*In this example, the template includes a **!** at the beginning. The **!** indicates that the inverse of the template is matched. Inverse matching can only be used with the match source template and requires a static target template (the target template cannot contain wildcards).*

For additional information about configuring SIP Diversion headers in SIP messaging, refer to the configuration guide, *Modifying SIP Headers on SIP Trunks in AOS Voice Products* available online at https://supportcommunity.adtran.com.

Usage Examples

In the following example, the SIP trunk (**t01**) is configured so that when the ANI source template (**2565558XXX**) is matched, an unconditional SIP Diversion header with a target template of **2565558000** and network screening and full privacy replaces the original SIP header.

(config)**#voice trunk t01**
(config-T01)**#match ani 2565558XXX replace diversion 2565558000 unconditional yes full**

match ani <*template*> substitute <*template*>

Use the **match ani substitute** command to configure automatic number identification (ANI) substitution for outbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

match ani <*template*> **substitute** <*template*>
match ani <*template*> **substitute** <*template*> **name** <*name*>

Syntax Description

ani <*template*>	Specifies the ANI information to be substituted. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the ANI information that is substituted for the original ANI information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
name <*name*>	Optional. Specifies the name associated with the ANI information. This option is only available on trunks that support ANI name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no ANI substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for ANI templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the ANI information from numbers **555-8111** to **555-8115** will be substituted by **555-8110** for outbound calls on the trunk **T03**:

(config)**#voice trunk t03 type sip**
(config-t03)**#match ani 555-811[125] substitute 555-8110**

match dnis <*template*> replace ani <*number*>

Use the **match dnis replace ani** command to replace dialed number identification service (DNIS) information with automatic number identification (ANI) information on outbound voice trunks. Use the **no** form of this command to remove the replacement. Variations of this command include:

match dnis <*template*> **replace ani** <*number*>
match dnis <*template*> **replace ani** <*number*> **name** <*name*>

Syntax Description

dnis <*template*>	Specifies the DNIS information to be replaced. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
replace ani <*number*>	Specifies the ANI information that replaces the original DNIS information. This information is entered using numerical digits. Enter the number without punctuation.
name <*name*>	Optional. Specifies the name associated with the ANI information. This option is only available on trunks that support ANI name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no DNIS replacement is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for DNIS templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits

3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the DNIS information for dialed numbers on trunk **T03** that match **1-256-524-8600** are replaced with **882-6467**:

(config)**#voice trunk t03 type sip**
(config-t03)**#match dnis 1-256-524-8600 replace ani 8826467**

match dnis <*template*> substitute <*template*>

Use the **match dnis substitute** command to configure dialed number identification service (DNIS) substitution for outbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

match dnis <*template*> **substitute** <*template*>
match dnis <*template*> **substitute** <*template*> **name** <*name*>

Syntax Description

dnis <*template*>	Specifies the DNIS information to be substituted. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the DNIS information that is substituted for the original DNIS information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
name <*name*>	Optional. Specifies the name associated with the DNIS information. This option is only available on trunks that support DNIS name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no DNIS substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for DNIS templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the DNIS information for dialed numbers on trunk **T03** that match **1-334-NXX-XXXX** are substituted with **1-800-557-4500**:

(config)**#voice trunk t03 type sip**
(config-t03)**#match dnis 1-334-NXX-XXXX substitute 1-800-557-4500**

max-number-calls <*value*>

Use the **max-number-calls** command to configure the maximum number of calls allowed on this trunk. This command is useful in controlling the call usage of the trunk. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies the maximum number of calls allowed on this trunk. Range is **1** to **64** calls.

Default Values

By default, no maximum number of calls is specified.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the maximum number of calls allowed to **25**:

(config)**#voice trunk t01 type sip**
(config-t01)**#max-number-calls 25**

media-loopback

Use the **media-loopback** command to configure a Session Initiation Protocol (SIP) trunk to allow media loopback calls to be placed on the trunk. Media loopback enables media sessions to be established where the media is looped back to the transmitter. This is typically referred to as active monitoring of services. This command allows media loopback sessions on some SIP trunks while disallowing media-loopback on others. Use the **no** form of this command do disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **media-loopback** is enabled on SIP trunks.

Command History

Release A4.03	Command was introduced.

Usage Examples

The following example enables media loopback on trunk **T01**:

(config)**#voice trunk t01 type sip**
(config-t01)**#media-loopback**

options-supported

Use the **options-supported** command to enable support for the OPTIONS message for calls on the trunk. Use the **no** form of this command to return to the default setting. Variations of this command include:

options-supported
options-supported forward

Syntax Description

forward	Optional. Enables support for forwarding in-dialog OPTIONS requests to the other trunk involved in a call.

Default Values

By default, this feature is enabled.

Command History

Release R13.8.0	Command was introduced.

Usage Examples

The following example enables support for OPTIONS messages for calls on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#options-supported**

outbound-proxy primary <*value*>

Use the **outbound-proxy primary** command to define the primary name/address of the Session Initiation Protocol (SIP) proxy server to which the trunk will send all SIP messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

outbound-proxy primary <*value*>
outbound-proxy primary <*value*> **tcp**
outbound-proxy primary <*value*> **tcp** <*port*>
outbound-proxy primary <*value*> **udp**
outbound-proxy primary <*value*> **udp** <*number*>
outbound-proxy primary <*value*> **tls** <*profile name*>
outbound-proxy primary <*value*> **tls** <*profile name*> **srv**
outbound-proxy primary <*value*> **tls** <*profile name*> **srv** <*service name prefix*>
outbound-proxy primary <*value*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
outbound-proxy primary <*value*> **tls** <*profile name*> <*port*>
outbound-proxy primary <*value*> **tls** <*profile name*> <*port*> **srv**
outbound-proxy primary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
outbound-proxy primary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
<*transport name prefix*>

Syntax Description

<*value*>	Specifies the fully qualified domain name (FQDN) or IP address of the outbound proxy server.
tcp	Optional. Sets the Transmission Control Protocol (TCP) port of the outbound proxy server.
udp	Optional. Sets the User Datagram Protocol (UDP) port of the outbound proxy server.
tls <*profile name*>	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<*port*>	Optional. Specifies the port number. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<*service name prefix*>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<*transport name prefix*>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, the IP address is set to **0.0.0.0**, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was expanded.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Functional Notes

The configured value must resolve to a valid IP address.

Usage Examples

The following example sets the outbound proxy server to **sip-proxy.adtran.com** with a UDP port of **2222**:

(config)**#voice trunk t01 type sip**
(config-t01)**#outbound-proxy primary sip-proxy.adtran.com udp 2222**

The following example specifies the SIP trunk as a primary SIP server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#voice trunk t01 type sip**
(config-t01)**#outbound-proxy primary 10.10.10.1 tls TLSPROFILE1**

outbound-proxy secondary <*value*>

Use the **outbound-proxy secondary** command to define the secondary name/address of the Session Initiation Protocol (SIP) proxy server to which the trunk will send all SIP messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

outbound-proxy secondary <*value*>
outbound-proxy secondary <*value*> **tcp**
outbound-proxy secondary <*value*> **tcp** <*port*>
outbound-proxy secondary <*value*> **udp**
outbound-proxy secondary <*value*> **udp** <*port*>
outbound-proxy secondary <*value*> **tls** <*profile name*>
outbound-proxy secondary <*value*> **tls** <*profile name*> **srv**
outbound-proxy secondary <*value*> **tls** <*profile name*> **srv** <*service name prefix*>
outbound-proxy secondary <*value*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
outbound-proxy secondary <*value*> **tls** <*profile name*> <*port*>
outbound-proxy secondary <*value*> **tls** <*profile name*> <*port*> **srv**
outbound-proxy secondary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
outbound-proxy secondary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*> <*transport name prefix*>

Syntax Description

<*value*>	Specifies the fully qualified domain name (FQDN) or IP address of the outbound proxy server.
tcp	Optional. Sets the Transmission Control Protocol (TCP) port of the outbound proxy server.
udp	Optional. Sets the User Datagram Protocol (UDP) port of the outbound proxy server.
tls <*profile name*>	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<*port*>	Optional. Specifies the port number. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<*service name prefix*>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<*transport name prefix*>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, the IP address is set to **0.0.0.0**, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release 15.1	Command was introduced.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Functional Notes

The configured value must resolve to a valid IP address.

Usage Examples

The following example sets the outbound proxy server to **sip-proxy.adtran.com** with a UDP port of **2244**:

(config)**#voice trunk t01 type sip**
(config-t01)**#outbound-proxy secondary sip-proxy.adtran.com udp 2244**

The following example specifies the SIP trunk as a secondary SIP server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#voice trunk t01 type sip**
(config-t01)**#outbound-proxy secondary 10.10.10.1 tls TLSPROFILE1**

p-assert-diversion

Use the **p-assert-diversion** command to enable sending P-Asserted-Identity in place of the Session Initiation Protocol (SIP) diversion header. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example enables P-Asserted-Identity in place of the SIP diversion header:

(config)**#voice trunk t01 type sip**
(config-t01)**#p-assert-diversion**

peer-certificate-identity *<string>*

Use the **peer-certificate-identity** command to configure a static string used in peer validation for Transport Layer Security (TLS). The value specified at the trunk is used by the TLS profile to match for validation (refer to the TLS profile command *validate identity on page 4887*). Use the **no** form of this command to remove the string from the trunk's configuration.

Syntax Description

<string>	Specifies, in text, the static string for the trunk to use in TLS peer identity validation.

Default Values

By default, no peer identity string is defined.

Command History

Release R11.5.0	Command was introduced.

Usage Examples

The following example defines a static string for use in TLS validation:

(config)**#voice trunk t01 type sip**
(config-t01)**#peer-certificate-identity PEER1VALID**

phone-context

Use the **phone-context** command to create an entry in the phone-context map. The phone-context map allows call context information to be preserved between the Session Initiation Protocol (SIP) server and the primary rate interface (PRI). Use the **no** form of this command to delete the configured entry. Variations of this command include the following:

phone-context <*string*> **plan** <*indicator*> **type** <*number*>
phone-context <*string*> **plan** <*indicator*> **type abbreviated**
phone-context <*string*> **plan** <*indicator*> **type international**
phone-context <*string*> **plan** <*indicator*> **type level0**
phone-context <*string*> **plan** <*indicator*> **type level1**
phone-context <*string*> **plan** <*indicator*> **type level2**
phone-context <*string*> **plan** <*indicator*> **type national**
phone-context <*string*> **plan** <*indicator*> **type network-specific**
phone-context <*string*> **plan** <*indicator*> **type subscriber**
phone-context <*string*> **plan** <*indicator*> **type unknown**
phone-context <*string*> **plan e164 type** <*number*>
phone-context <*string*> **plan e164 type abbreviated**
phone-context <*string*> **plan e164 type international**
phone-context <*string*> **plan e164 type level0**
phone-context <*string*> **plan e164 type level1**
phone-context <*string*> **plan e164 type level2**
phone-context <*string*> **plan e164 type national**
phone-context <*string*> **plan e164 type network-specific**
phone-context <*string*> **plan e164 type subscriber**
phone-context <*string*> **plan e164 type unknown**
phone-context <*string*> **plan private type** <*number*>
phone-context <*string*> **plan private type abbreviated**
phone-context <*string*> **plan private type international**
phone-context <*string*> **plan private type level0**
phone-context <*string*> **plan private type level1**
phone-context <*string*> **plan private type level2**
phone-context <*string*> **plan private type national**
phone-context <*string*> **plan private type network-specific**
phone-context <*string*> **plan private type subscriber**
phone-context <*string*> **plan private type unknown**
phone-context <*string*> **plan unknown type** <*number*>
phone-context <*string*> **plan unknown type abbreviated**
phone-context <*string*> **plan unknown type international**
phone-context <*string*> **plan unknown type level0**
phone-context <*string*> **plan unknown type level1**
phone-context <*string*> **plan unknown type level2**
phone-context <*string*> **plan unknown type national**
phone-context <*string*> **plan unknown type network-specific**
phone-context <*string*> **plan unknown type subscriber**

phone-context <*string*> **plan unknown type unknown**

Syntax Description

<*string*>		Specifies a string of text for the phone-context map entry. This is used to convert between phone-context and NPI/TON values.
plan		Specifies the NPI to associate with the phone-context map entry.
	<*number*>	Specifies the NPI value. Valid range is **0** to **15**.
	e164	Specifies using the ISDN/telephone numbering plan (E.164) value (0001) for the NPI bits of the Type-of-Address octet.
	private	Specifies using the **private** numbering plan value (1001) for the NPI bits of the Type-of-Address octet.
	unkown	Specifies using the **unknown** numbering plan value (0000) for the NPI bits of the Type-of-Address octet.
type		Specifies the TON to associate with the phone-context map entry.
	<*number*>	Specifies the TON value. Valid range is **0** to **7**.
	abbreviated	Specifies using the **abbreviated** value (110) for the TON bits of the Type-of-Address octet. Abbreviated is used mainly in private ISDN network applications and the implementation is network dependent.
	international	Specifies using the **international** value (001) for the TON bits of the Type-of-Address octet. International is used for calls destined outside the national calling area. International calls have the international direct dialing (IDD) prefix removed. For example, consider an international call of 011-N$, where the IDD prefix is 011 and the N$ represents the digits necessary for routing the call at the destination. When the called party information element (IE) is created for this call, the prefix is stripped and the N$ digits are placed in the number digits field.
	level0	Specifies using the level 0 local number type in a Private Numbering Plan (PNP). The value of the TON bits of the Type-of-Address octet is identical to the **subscriber** value (100) in E.164 format.
	level1	Specifies using the level 1 regional number type in a PNP. The value of the TON bits of the Type-of-Address octet is identical to the **national** value (010) in E.164 format.
	level2	Specifies using the level 2 local number type in a PNP. The value of the TON bits of the Type-of-Address octet is identical to the **international** value (001) in E.164 format.
	national	Specifies using the **national** value (010) for the TON bits of the Type-of-Address octet. National is used for calls destined for inside the national calling area (calls that do not cross into an international local access and transport area (LATA)). National calls have the direct dialing prefix removed. For example, consider a national call with a direct dialing prefix of 1 and NXX-NXX-XXXX to represent the ten-digit number necessary for routing the call. When the called party IE is created for this call, the prefix (1) is stripped and the NXX-NXX-XXXX digits are placed in the number digits field.

network-specific	Specifies using the **network-specific** value (011) for the TON bits of the Type-of-Address octet. Network specific is used for calls that require special access to a private network, which requires the use of a prefix that should be stripped once access to the network has been gained. Network-specific calls have the dialing prefix removed. For example, a call to a private network with the prefix 700 consists of 700-N$, where 700 is the dialing prefix and N$ represents the digits necessary for routing the call at the destination. When the called party IE is created for this call, the prefix is stripped and the N$ is placed in the Number Digits field.
subscriber	Specifies using the **subscriber** value (100) for the TON bits of the Type-of-Address octet. Subscriber is used for local calls (not long distance). Subscriber calls, by default, have the area code removed. For example, a subscriber call to 916-555-1212 would have the prefix 916 stripped and 555-1212 in the number digits field. For areas with mandatory ten-digit dialing, a blank prefix should be entered to ensure that all ten digits are passed to the number digits field.
unknown	Specifies using the **unknown** value (000) for the TON bits of the Type-of-Address octet. Unknown is used when the number type is not known. Unknown numbers are presumed to have no prefix, and the entire dialed number is presented in the number digits field.

Default Values

By default, no phone-context map entries are configured.

Command History

Release R10.1.0	Command was introduced.

Functional Notes

During ISDN call establishment on a PRI, each phone number in the SETUP message is qualified with a pair of identifiers, TON and NPI, which determine how the phone number is to be treated. The mechanism by which a SIP server communicates information about phone numbers is the SIP URI phone-context field.

The **phone-context** command allows a table to be configured that stores associations between the SIP URI phone-context strings and NPI/TON value pairs. This map allows the SIP trunk to convert between numerical NPI/TON value pairs and a phone-context text string. Consequently, phone number information is preserved during interworking between SIP and ISDN PRI.

In the PRI to SIP direction, the received NPI/TON values are passed through the switchboard to the SIP trunk. The SIP trunk then uses the phone-context table to find the corresponding phone-context text string, and the string is inserted as a **phone-context=** parameter into the outgoing SIP URI.

In the SIP to PRI direction, the SIP trunk uses the phone-context table to convert the string received in the **phone-context=** parameter to the corresponding NPI/TON values. The values are then passed through the switchboard to the PRI trunk and on to the connected equipment.

Usage Examples

The following example creates an entry in the phone-context map that associates the phone-context string **phonesystem.adtran.com** with the **private** NPI and **level0** TON:

(config)**#voice trunk t01 type sip**
(config-t01)**#phone-context phonesystem.adtran.com plan private type level0**

prefer double-reinvite

Use the **prefer double-reinvite** command to specify that Session Initiation Protocol (SIP) double reInvite messages are included in calls involving the trunk. Calls that typically require a double reInvite are forwarded calls from call overage and any attended transfer, and when these calls connect, a double reInvite message is initiated when the feature is enabled. Using the **no** form of this command indicates that double reInvites are not preferred on the trunk. Use the command *sip prefer double-reinvite on page 1726* to specify the global setting for this feature. Variations of this command include:

prefer double-reinvite
prefer double-reinvite system

This command should only be issued by advanced users or at the direction of Adtran technical support.

Syntax Description

system	Optional. Specifies that the system double reInvite setting is used. The system setting is specified using the command *prefer double-reinvite on page 5113*.

Default Values

By default, all trunk accounts prefer a double re-Invite.

Command History

Release A5.01	Command was introduced.

Functional Notes

The **prefer double-reinvite** command is used in the trunk's configuration to determine whether a double reInvite is preferred in calls involving the trunk. By default, the system is configured so that double reInvites are preferred, and all trunk accounts prefer a double reInvite. Double reInvites are used, for example, when a SIP trunk in local transfer mode is providing ring-back during a blind transfer. In this scenario, a double reInvite must occur in order to establish a talk path after the transfer target answers.

You can also specify whether Session Description Protocol (SDP) is used in the double reInvite message. To send a double reInvite without SDP, refer to the command *prefer reinvite-without-sdp on page 5114*. This command helps determine which endpoint receives SDP in the double reInvite call flow.

Usage Examples

The following example specifies that SIP double reInvites are not preferred on this trunk:

(config)**#voice trunk t01 type sip**
(config-t01)**#no prefer double-reinvite**

prefer reinvite-without-sdp

Use the **prefer reinvite-without-sdp** command to specify that Session Initiation Protocol (SIP) double reInvite messages are included in calls involving the trunk, but that these messages do not include Session Description Protocol (SDP). This command helps to determine which endpoint receives the SDP in the double reInvite call flow. Using the **no** form of this command indicates that reInvite messages without SDP are not preferred. Use the command *sip prefer double-reinvite on page 1726* to specify the global setting for this feature.

This command should only be issued by advanced users or at the direction of Adtran technical support.

Syntax Description

No subcommands.

Default Values

By default, all trunk accounts prefer a double reInvite with SDP.

Command History

Release A5.01	Command was introduced.

Functional Notes

When a double reInvite is initiated, the first reInvite without SDP is not sent to the account that does not require it. When both accounts do not require a reInvite with SDP, the target account sends the initial reInvite message.

You can specify whether a re-Invite is preferred on the trunk using the command *prefer double-reinvite on page 5113*. This command is used in the trunk's configuration to determine whether a double reInvite is preferred in calls involving the trunk. By default, the system is configured so that double reInvites are preferred, and all trunk accounts prefer a double reInvite. Double reInvites are used, for example, when a SIP trunk in local transfer mode is providing ring-back during a blind transfer. In this scenario, a double reInvite must occur in order to establish a talk path after the transfer target answers.

Usage Examples

The following example specifies that SIP double reInvites with SDP are preferred on this trunk:

(config)**#voice trunk t01 type sip**
(config-t01)**#no prefer reinvite-without-sdp**

prefer trunk-routing

Use the **prefer trunk-routing** command to add a trunk to a list of trunks that are considered first for call routing, regardless of system routing mode or locally configured extensions. Use the **no** form of this command to remove the trunk from the list.

Syntax Description

No subcommands.

Default Values

By default, **prefer trunk-routing** is disabled.

Command History

Release A2	Command was introduced.

Functional Notes

Trunk routing can be specified as a preference for specific trunks, allowing the trunk to be considered first for routing rather than relying on the internal or external nature of the call to dictate whether the trunk or voice station is the first choice routing path. The **prefer trunk-routing** command, executed from a specific trunk's configuration mode, adds the trunk to a list of trunks that are considered first for routing.

By default, no trunk routing preference is set, so that each trunk operates as dictated by normal call routing modes. Adding the trunk routing preference only affects how inbound calls from the specific trunk are handled.

Usage Examples

The following example specifies that trunk routing is preferred on the trunk **T01**:

(config)**#voice trunk t01 type sip**
(config-t01)**#prefer trunk-routing**

reason-supported

Use the **reason-supported** command to enable support for the addition of Session Initiation Protocol (SIP) Reason headers to outgoing SIP requests on the trunk. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R13.8.0	Command was introduced.

Usage Examples

The following example enables the addition of SIP Reason headers to outgoing SIP requests on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#reason-supported**

register

Use the **register** command to define the Session Initiation Protocol (SIP) name for registration of the authorization name(s) and password(s). Use the **no** form of this command to remove a registration. Variations of this command include the following:

register <*name*>
register <*name*> **auth-name** <*username*> **password** <*word*>
register range <*begin*> <*end*>
register range <*begin*> <*end*> **auth-name** <*username*> **password** <*word*>
register range <*begin*> <*end*> **auth-name range** <*begin*> <*end*> **password range** <*begin*> <*end*>
register range <*begin*> <*end*> **auth-name range** <*begin*> <*end*> **password** <*word*>

When using the range option, there must be the same number of elements in each related range. In other words, each SIP user in a range must have one authentication name and/or one password.

Syntax Description

<*name*>	Specifies the name of the SIP trunk to register.
range <*begin*> <*end*>	Specifies the beginning and ending of the range to register SIP users, authentication names, and/or passwords.
auth-name <*username*>	Optional. Specifies the user name for authentication.
password <*word*>	Optional. Specifies the password for authentication.

Default Values

By default, no registration range is programmed.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was expanded.

Functional Notes

Using the **range** option reduces the time required to program individual user registration and authentication settings. The range configuration option allows multiple users to be configured in one step for example:

register range 2565553000 2565553100 auth-name range Adtran3000 Adtran3100 password range adtn3000 adtn3100

In this example, 100 users in the range (256) 555-3000 to (256) 555-3100 are registered with authentication names ranging from **Adtran3000** to **Adtran3100** and passwords ranging from **adtn3000** to **adtn3100**.

The user may enter an authentication name range, password range, or both. An error will be returned if the provided authentication name and/or password range values are not large enough for the SIP identity range provided (i.e., in the example, if the user had entered Adtran3000 Adtran3099 for the authentication name range, an error would have been returned because the specified SIP identity range is 100 users (not 99)).

Usage Examples

The following example registers trunk **T01** under the name of **MainOffice**:

(config)**#voice trunk t01 type sip**
(config-t01)**#register MainOffice**

The following example sets the authorization name and password range for a group of SIP users:

(config)**#voice trunk t01 type sip**
(config-t01)**#register range 2565554000 2565554100 auth-name range Adtran4000 Adtran4100 password range adtn8000 adtn8100**

registrar expire-time <*value*>

Use the **registrar expire-time** command to define the Session Initiation Protocol (SIP) expiration time for requested registration. This command specifies the duration of the registration that is requested in the REGISTER sent to the SIP server. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies expiration time (in seconds) for a registration. Valid range depends on whether the command *registrar threshold on page 5126* is configured for **absolute** or **percentage**. If the threshold is set to **percentage**, the range is **0** to **4294967295**. If the threshold is set to **absolute**, the range is <*absolute threshold value*> **+ 6** to **4294967295**.

Default Values

By default, this value is set to **3600** seconds.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example specifies the registration expiration time for the SIP trunk as **1800** seconds:

(config)**#voice trunk t01 type sip**
(config-t01)**#registrar expire-time 1800**

registrar max-concurrent-reg <*value*>

Use the **registrar max-concurrent-reg** command to control the maximum number of simultaneous registration requests that are allowed for the trunk. This value can be adjusted to help eliminate congestion caused by too many concurrent registration requests. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the maximum number of concurrent registrations. Valid range is **1** to **32** registrations.

Default Values

By default, the maximum number of concurrent registrations is set to **32**.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example sets the maximum number on concurrent registrations to **12**:

(config)**#voice trunk t01 type sip**
(config-t01)**#registrar max-concurrent-reg 12**

registrar primary <*value*>

Use the **registrar primary** command to define the primary Session Initiation Protocol (SIP) registrar fully qualified domain name (FQDN) or IP address that is based on the domain naming system (DNS) suffix. Use the **no** form of this command to return to the default setting. Variations of this command include:

registrar primary <*value*>
registrar primary <*value*> **tcp**
registrar primary <*value*> **tcp** <*port*>
registrar primary <*value*> **udp**
registrar primary <*value*> **udp** <*port*>
registrar primary <*value*> **tls** <*profile name*>
registrar primary <*value*> **tls** <*profile name*> **srv**
registrar primary <*value*> **tls** <*profile name*> **srv** <*service name prefix*>
registrar primary <*value*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
registrar primary <*value*> **tls** <*profile name*> <*port*>
registrar primary <*value*> **tls** <*profile name*> <*port*> **srv**
registrar primary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
registrar primary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*> <*transport name prefix*>

A secondary SIP registrar can be set using the command *registrar secondary <value> on page 5124*.

Syntax Description

<*value*>	Specifies the FQDN or IP address of the registrar server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
tcp	Optional. Sets the Transmission Control Protocol (TCP) port of the registrar server.
udp	Optional. Sets the User Datagram Protocol (UDP) port of the registrar server.
tls <*profile name*>	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<*port*>	Optional. Specifies the port number. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<*service name prefix*>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<*transport name prefix*>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, the IP address is set to **0.0.0.0**, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was expanded.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Functional Notes

This command specifies which trunk will send SIP register messages. The configured value must resolve to a valid IP address.

Usage Examples

The following example sets the registrar server to **as1.adtran.com** with a UDP port of **9060**:

(config)**#voice trunk t01 type sip**
(config-t01)**#registrar primary as1.adtran.com udp 9060**

The following example specifies the SIP trunk as a primary SIP registrar server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#voice trunk t01 type sip**
(config-t01)**#registrar primary 10.10.10.1 tls TLSPROFILE1**

registrar require-expires

Use the **registrar require-expires** command to define the Session Initiation Protocol (SIP) expiration time for registration. A successful response to a register contains an expires header or the response is considered a failure. When disabled, a successful response does not require an expires header to be considered successful. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specifies expiration time (in seconds) for a response to a registration request.

Default Values

By default, the registration expiration time is enabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example disables registration expiration time for the SIP trunk:

(config)**#voice trunk t01 type sip**
(config-t01)**#no registrar require-expires**

registrar secondary <*value*>

Use the **registrar secondary** command to define the primary Session Initiation Protocol (SIP) registrar fully qualified domain name (FQDN) or IP address that is based on the domain naming system (DNS) suffix. Use the **no** form of this command to return to the default setting. Variations of this command include:

registrar secondary <*value*>
registrar secondary <*value*> **tcp**
registrar secondary <*value*> **tcp** <*port*>
registrar secondary <*value*> **udp**
registrar secondary <*value*> **udp** <*port*>
registrar secondary <*value*> **tls** <*profile name*>
registrar secondary <*value*> **tls** <*profile name*> **srv**
registrar secondary <*value*> **tls** <*profile name*> **srv** <*service name prefix*>
registrar secondary <*value*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
registrar secondary <*value*> **tls** <*profile name*> <*port*>
registrar secondary <*value*> **tls** <*profile name*> <*port*> **srv**
registrar secondary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
registrar secondary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*> <*transport name prefix*>

Syntax Description

<*value*>	Specifies the FQDN or IP address of the registrar server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
tcp	Optional. Sets the Transmission Control Protocol (TCP) port of the registrar server.
udp	Optional. Sets the User Datagram Protocol (UDP) port of the registrar server.
tls <*profile name*>	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<*port*>	Optional. Specifies the port number. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<*service name prefix*>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<*transport name prefix*>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, the IP address is set to **0.0.0.0**, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was expanded.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Functional Notes

This command specifies which trunk will send SIP register messages. The configured value must resolve to a valid IP address.

Usage Examples

The following example sets the secondary registrar server to **as1.adtran.com** with a UDP port of **9060**:

(config)**#voice trunk t01 type sip**
(config-t01)**#registrar secondary as1.adtran.com udp 9060**

The following example specifies the SIP trunk as a secondary SIP registrar server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#voice trunk t01 type sip**
(config-t01)**#registrar secondary 10.10.10.1 tls TLSPROFILE1**

registrar threshold

Use the **registrar threshold** command to specify the Session Initiation Protocol (SIP) trunk registration renewal threshold. Use the **no** form of this command to return to the default value. Variations of this command include:

registrar threshold absolute <*value*>
registrar threshold percentage <*percent*>

Syntax Description

absolute <*value*>	Specifies that the registration renewal occurs when the remaining amount of time on the registration coincides with this value. Valid range is **5** to **604800** seconds (1 week).
percentage <*percent*>	Specifies that the renewal occurs at a certain remaining percentage of the registration time. Valid range is **1** to **90** percent.

Default Values

By default, the registrar threshold is set at **absolute 300** seconds.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example sets the registrar renewal threshold time at **50** percent of the returned valid registration time:

(config)**#voice trunk t01 type sip**
(config-t01)**#registrar threshold percentage 50**

reject-external

Use the **reject-external** command to prevent inbound calls on the trunk from being routed back out of the same trunk. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Functional Notes

In general, trunks are assigned to the user role, which means they terminate lines from a Telco provider. If this is the case, **reject-external** should be enabled so that inbound calls on the trunk cannot be routed back out of the same trunk. If the configuration is poor, inbound long distance calls could be routed back out of the same trunk, causing the owner of the unit to be charged for long distance calls without his knowledge. For network-role trunks and SIP-based trunks, this command should be disabled to allow calls to be properly routed in the unit.

Usage Examples

The following example activates **reject-external**:

(config)**#voice trunk t01 type sip**
(config-t01)**#reject-external**

require-registration *<identity>*

Use the **require-registration** command to allow registration for one Private Branch Exchange (PBX) on the Session Initiation Protocol (SIP) trunk. Use the **no** form of this command to disable the feature. Variations of this command include:

require-registration *<identity>*
require-registration *<server>* **auth-name** *<username>* **password** *<password>*

Syntax Description

<identity>	Specifies the identity of the SIP user used for registration.
auth-name *<username>* **password** *<password>*	Optional. Specifies a user name and password for registration authentication.

Default Values

By default, this feature is disabled.

Command History

Release R13.8.0	Command was introduced.

Functional Notes

When PBX registration is enabled on the trunk, the following conditions occur:

- INVITE requests received from an unregistered PBX result in a response code of 403.
- When enabled in tandem with the SIP Reason header addition feature (refer to the command *reason-supported on page 5116*), INVITE requests from the WAN interface to an unregistered PBX result in a response code of 480 and a Reason header containing Q.850 Cause number 18.
- Failure of PBX to register before the expires time sent by the AOS registrar elapses will result in the PBX being considered unregistered.
- A valid registration request from a registered PBX will renew the registration time period.
- SIP registrar authentication must also be enabled for PBX registration requests to be issued an authentication challenge. If the specified user name or password contained in the Authorization header of the PBX registration request do not match what is specified in the SIP registrar authentication configuration, the registration request is rejected.

Usage Examples

The following example enables PBX registration on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#require-registration 2565551234**

ringback override

Use the **ringback** command to specify ringback options for calls on the trunk. Use the **no** form of this command to return to the default setting. Variations of this command include:

ringback override 180
ringback override 183

Syntax Description

180	Specifies override a 180 and send 183 with local ringback.
183	Specifies override a 183 and send 183 with local ringback.

Default Values

By default, no ringback override is specified.

Command History

Release A5.03	Command was introduced.

Usage Examples

The following example enables ringback override 180 and 183 on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#ringback override 180**
(config-t01)**#ringback override 183**

rtp dtmf-relay offer

Use the **rtp dtmf-relay offer** command to specify which dualtone multifrequency (DTMF) relay mode to offer to a particular Session Initiation Protocol (SIP) endpoint when using DTMF transcoding. Use the **no** form of this command to return the DTMF method to default value. Variations of this command include:

rtp dtmf-relay offer inband
rtp dtmf-relay offer nte <*value*>

Syntax Description

inband	Specifies that the DTMF relay method is in-band.
nte <*value*>	Specifies that the DTMF relay method is an RFC 2833 named telephone events (NTE). Valid NTE value range is **96** to **127**.

Default Values

By default, there is no preferred DTMF relay mode on the SIP endpoint, and the Session Border Controller (SBC) can choose a DTMF value that does not require transcoding to complete a call.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

The **rtp dtmf-relay offer** command is used to enable and configure DTMF transcoding on the AOS device when it is acting as an SBC. Transcoding is a method of translating media types in which the SBC operates as a translator for SIP devices using different media types that are attempting a connection. The AOS device translates one media type to another to allow the communication to succeed. For more information about transcoding and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

Before you can configure the DTMF relay method for transcoding, you must enable media anchoring using the command *ip rtp media-anchoring on page 1458*.

Usage Examples

The following example specifies the NTE 101 DTMF relay method for transcoding on the SIP trunk:

(config)**#ip rtp media-anchoring transcoding dtmf**
(config)**#voice trunk T01 type sip**
(config-T01)**#rtp dtmf-relay offer nte 101**

rtp media video filter

Use the **rtp media video filter** command to filter out video media attributes from transmitted or received Session Description Protocol (SDP) messages on an AOS device acting as a session border controller (SBC). You can filter out video media on a Session Initiation Protocol (SIP) endpoint by entering the command from the SIP endpoint's configuration mode. Use the **no** form of this command to disable the media filtering feature.

Syntax Description

No subcommands.

Default Values

By default, media filtering is disabled and all video SDP media attributes are passed through the SBC device.

Command History

Release R10.4.0	Command was introduced.

Functional Notes

Media filtering is a part of the transcoding feature that is available when the AOS device is acting as an SBC. For more information about transcoding and the media filtering feature, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportofurms.adtran.com.

Usage Examples

The following example enables media filtering on the voice trunk:

(config)**#voice trunk T01 type sip**
(config-T01)**#rtp media video filter**

sip-header-passthrough

Use the **sip-header-passthrough** command to enable and configure Session Initiation Protocol (SIP) header transparency on the trunk. Use the **no** form of this command to disable the feature. Variations of this command include:

sip-header-passthrough both
sip-header-passthrough in
sip-header-passthrough out

Syntax Description

both	Enables support for SIP header transparency for both inbound and outbound messages.
in	Enables support for SIP header transparency for inbound messages.
out	Enables support for SIP header transparency for outbound messages.

Default Values

By default, this feature is disabled.

Command History

Release R13.8.0	Command was introduced.

Usage Examples

The following example enables support for SIP header transparency for inbound messages on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-header-passthrough in**

sip-keep-alive

Use the **sip-keep-alive** command to configure the type of keep-alive method for this Session Initiation Protocol (SIP) trunk. Keep-alive messages must be sent between SIP device and the registrar to keep the connected channel open for communication. Use the **no** form of this command to return to disable this feature. Variations of this command include the following:

sip-keep-alive info
sip-keep-alive info <*value*>
sip-keep-alive options
sip-keep-alive options <*value*>

Syntax Description

info	Specifies the INFO method to be used for the keep-alives on the trunk.
options	Specifies the OPTIONS method to be used for the keep-alives on the trunk.
<*value*>	Optional. Specifies the amount of time in seconds between the type of SIP keep-alive messages being sent during a call. Range is **30** to **3600** seconds.

Default Values

By default, **sip-keep-alive** is set to **info 60** on NetVanta 7000 Series products. For IP business gateways (Total Access 900(e) Series and NetVanta 6000 Series) **sip-keep-alive** is disabled by default.

Command History

Release 13.1	Command was introduced
Release A2.04	Command was added to the Voice Line and Voice User command sets.

Usage Examples

The following example sets the keep-alive method to **info**:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-keep-alive info**

sip-server primary <*value*>

Use the **sip-server primary** command to define the primary name/address of the Session Initiation Protocol (SIP) server to which the trunk will send call-related SIP messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip-server primary <*value*>
sip-server primary <*value*> **tcp**
sip-server primary <*value*> **tcp** <*port*>
sip-server primary <*value*> **udp**
sip-server primary <*value*> **udp** <*port*>
sip-server primary <*value*> **tls** <*profile name*>
sip-server primary <*value*> **tls** <*profile name*> **srv**
sip-server primary <*value*> **tls** <*profile name*> **srv** <*service name prefix*>
sip-server primary <*value*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
sip-server primary <*value*> **tls** <*profile name*> <*port*>
sip-server primary <*value*> **tls** <*profile name*> <*port*> **srv**
sip-server primary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
sip-server primary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
<*transport name prefix*>

Syntax Description

<*value*>	Specifies the FQDN or IP address of the server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
tcp	Optional. Sets the Transmission Control Protocol (TCP) port of the server.
udp	Optional. Sets the User Datagram Protocol (UDP) port of the server.
tls <*profile name*>	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<*port*>	Optional. Specifies the port number. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<*service name prefix*>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<*transport name prefix*>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, the IP address is set to **0.0.0.0**, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was expanded.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Usage Examples

The following example sets the SIP proxy server to **as1.adtran.com** with a UDP port of **9060**:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-server primary as1.adtran.com udp 9060**

The following example specifies the SIP trunk as a primary SIP server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-server primary 10.10.10.1 tls TLSPROFILE1**

sip-server rollover

Use the **sip-server rollover** command to configure the rollover behavior of the Session Initiation Protocol (SIP) server. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip-server rollover service-unavailable-or-timeout
sip-server rollover timeout-only

Syntax Description

service-unavailable-or-timeout	Specifies the rollover to the next SIP server to occur after receiving a 503 Service Unavailable message or no response.
timeout-only	Specifies the rollover to the next SIP server to occur only after no response is received.

Default Values

By default, the **sip-server rollover** is set to **timeout-only**.

Command History

Release A2.03	Command was introduced.

Usage Examples

The following example sets the SIP server rollover to **timeout-only**:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-server rollover timeout-only**

sip-server secondary <*value*>

Use the **sip-server secondary** command to define the secondary name/address of the Session Initiation Protocol (SIP) server to which the trunk will send call-related SIP messages. Use the **no** form of this command to return to the default setting. Variations of this command include:

sip-server secondary <*value*>
sip-server secondary <*value*> **tcp**
sip-server secondary <*value*> **tcp** <*port*>
sip-server secondary <*value*> **udp**
sip-server secondary <*value*> **udp** <*port*>
sip-server secondary <*value*> **tls** <*profile name*>
sip-server secondary <*value*> **tls** <*profile name*> **srv**
sip-server secondary <*value*> **tls** <*profile name*> **srv** <*service name prefix*>
sip-server secondary <*value*> **tls** <*profile name*> **srv** <*service name prefix*> <*transport name prefix*>
sip-server secondary <*value*> **tls** <*profile name*> <*port*>
sip-server secondary <*value*> **tls** <*profile name*> <*port*> **srv**
sip-server secondary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
sip-server secondary <*value*> **tls** <*profile name*> <*port*> **srv** <*service name prefix*>
<*transport name prefix*>

Syntax Description

<*value*>	Specifies the FQDN or IP address of the registrar server. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
tcp	Optional. Sets the Transmission Control Protocol (TCP) port of the server.
udp	Optional. Sets the User Datagram Protocol (UDP) port of the server.
tls <*profile name*>	Optional. Associates a Transport Layer Security (TLS) profile with the trunk, thus specifying the TLS operation on the trunk.
<*port*>	Optional. Specifies the port number. Range is **0** to **65535**.
srv	Optional. Specifies that service records (SRV) parameters are enabled. This option is available only when an FQDN has been specified.
<*service name prefix*>	Optional. Specifies the service name used to format the domain naming service (DNS) SRV request used to resolve the domain name. Underscores are added automatically.
<*transport name prefix*>	Optional. Specifies the transport name used to format the DNS SRV request used to resolve the domain name. Underscores are added automatically.

Default Values

By default, the IP address is set to **0.0.0.0**, the UDP port is set to **5060**, and the TLS port is set to **5061**.

Command History

Release 9.3	Command was introduced.
Release 15.1	Command was expanded.
Release R11.5.0	Command was expanded to include the TLS and SRV configuration options.

Usage Examples

The following example sets the SIP proxy server to **as1.adtran.com** with a UDP port of **9070**:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-server secondary as1.adtran.com udp 9070**

The following example specifies the SIP trunk as a secondary SIP server at IP address **10.10.10.1** using TLS profile **TLSPROFILE1** on the default port:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-server secondary 10.10.10.1 tls TLSPROFILE1**

sip-server triggered-registration

Use the **sip-server triggered-registration** command to enable the Session Initiation Protocol (SIP) triggered registration feature on the trunk. Use the **no** form of this command to disable the feature.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R13.8.0	Command was introduced.

Usage Examples

The following example enables the SIP triggered registration feature on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#sip-server triggered-registration**

sip-server validation register

Use the **sip-server validation register** command to enable Session Initiation Protocol (SIP) server validation on the trunk for use in SIP trunk failover. When this feature is enabled, new REGISTER requests are only sent to valid servers, or the highest priority server to which the SIP trunk can register. Use the **no** form of this command to disable the validation feature.

Syntax Description

No subcommands.

Default Values

By default, SIP server validation is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

Enabling this feature configures the trunk to use the validated form of SIP trunk failover. This method of SIP trunk failover works in this manner:

When the AOS unit first boots, it establishes a prioritized list of SIP server addresses, using DNS as necessary. It uses the highest priority server as the destination of outbound trunk registrations. As long as these registrations are successful, the unit continues to use that server. If a failover condition occurs (if a request times out or there is no response from the server), the unit unregisters the specific registration to that server. The unit then iterates through the prioritized list of servers to find a valid one. A server is valid if it accepts the trunk registration request. All other trunk registrations remain unchanged. When the registration expires, the new REGISTER request is always sent to the highest priority server address in the list.

Usage Examples

The following example enables SIP server validation for the trunk:

```
(config)#voice trunk t01 type sip
(config-t01)#sip-server validation register
```


snmp trap registration failures <*value*> interval <*value*>

Use the **snmp trap registration** command to specify that Simple Network Management Protocol (SNMP) traps are enabled for the trunk, and that these traps are sent for Session Initiation Protocol (SIP) registration events. In addition, this command specifies how many registration failures can occur before an SNMP trap is sent, and at what interval the traps are sent. Use the **no** form of this command to disable SNMP traps for the trunk.

Syntax Description

failures <*value*>	Specifies the number of failures that occur before a trap is sent. Valid range is **1** to **128** failures.
interval <*value*>	Specifies the time (in seconds) that elapses between traps. Valid range is **30** to **86400** seconds.

Default Values

By default, SNMP traps are disabled on the trunk.

Command History

Release A5.01	Command was introduced.

Usage Examples

The following example enables SNMP traps on the trunk, and specifies that traps are sent for every **3** registration failures and every **3600** seconds:

(config)**#voice trunk t01 type sip**
(config-t01)**#snmp trap registration failures 3 interval 3600**

srtp *<profile name>*

Use the **srtp** *<profile name>* command to enable Secure Realtime Transfer Protocol (SRTP) on the Session Initiation Protocol (SIP) trunk and to associate an SRTP profile with the trunk. Use the **no** form of this command to disable SRTP on the trunk. Variations of this command include:

srtp *<profile name>*
srtp allow-non-rtp-media *<profile name>*
srtp allow-non-rtp-media reduced-rekeying roc-reset-on-reinvite *<profile name>*
srtp allow-non-rtp-media tls-optional *<profile name>*
srtp allow-non-rtp-media tls-optional reduced-rekeying roc-reset-on-reinvite *<profile name>*
srtp optional avp *<profile name>*
srtp optional avp reduced-rekeying roc-reset-on-reinvite *<profile name>*
srtp optional avp tls-optional *<profile name>*
srtp optional avp tls-optional reduced-rekeying roc-reset-on-reinvite *<profile name>*
srtp optional avp-savp *<profile name>*
srtp optional avp-savp reduced-rekeying roc-reset-on-reinvite *<profile name>*
srtp optional avp-savp tls-optional *<profile name>*
srtp optional avp-savp tls-optional reduced-rekeying roc-reset-on-reinvite *<profile name>*
srtp reduced-rekeying roc-reset-on-reinvite *<profile name>*
srtp tls-optional *<profile name>*
srtp tls-optional reduced-rekeying roc-reset-on-reinvite *<profile name>*

Syntax Description

<profile name>	Specifies the name of the SRTP profile to associate with the trunk. This profile must be specified as it sets the rules for SRTP use on the trunk.
allow-non-rtp-media	Optional. Configures SRTP to allow non-Realtime Transport Protocol (RTP) media, such as T.38 over UDPTL, that cannot be protected by SRTP. When this option is specified, RTP media is secured by SRTP, but any non-RTP media is forwarded unsecured.
reduced-rekeying	Optional. Specifies that SRTP rekeying on reINVITES will be disabled if the received SDP offer is unchanged.
roc-reset-on-reinvite	Optional. Specifies that AOS will reset the outbound rollover counter (ROC) when it sends a reINVITE.
tls-optional	Optional. Specifies that Session Description Protocol Security Descriptions (SDES) negotiation of SRTP is permitted over an unsecure control channel (NOT RECOMMENDED). If this option is not set, the control channel must be secured by Transport Layer Security (TLS) in order to perform SDES negotiation.
optional avp	Optional. Specifies that if negotiation permits, fall back to RTP audio video profile (AVP) is allowed. If this option is not specified, SRTP must be used for negotiation or the call fails.
optional avp-savp	Optional. Specifies that if negotiation permits, fall back to RTP AVP or secure AVP (SAVP) is allowed. If this option is not specified, SRTP must be used for negotiation or the call fails.

Default Values

By default, SRTP is not enabled on the trunk. If SRTP is enabled on the trunk, then by default, SRTP re-keying is enabled.

Command History

Release R11.5.0	Command was introduced.
Release R13.1.0	Command was expanded to include the **allow-non-rtp-media** parameter.
Release R13.4.0	Command was expanded to include the **reduced-rekeying** parameter.
Release R13.7.0	Command was expanded to include the **roc-reset-on-reinvite** parameter.

Functional Notes

Media anchoring must be enabled for SRTP to function.

Usage Examples

The following example specifies the trunk uses SRTP negotiation and TLS control channel security with SRTP profile **SRTPPROFILE1**:

(config)**#voice trunk t01 type sip**
(config-t01)**#srtp SRTPPROFILE1**

subscribe message-summary

Use the **subscribe** command to enable delivery of message-summary for successful registrations on the trunk. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release R10.10.0	Command was introduced.

Usage Examples

The following example enables sending the message-summary for successful registrations on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#subscribe message-summary**

subscribe rfc-3680-event-package

Use the **subscribe rfc-3680-event-package** command to enable subscription to RFC 3680 event packages for successful registrations on the trunk. Use the **no** form of this command to return to the default setting. Variations of this command include:

subscribe rfc-3680-event-package deregister-on-termination
subscribe rfc-3680-event-package expire-time <*value*>
subscribe rfc-3680-event-package threshold absolute <*value*>
subscribe rfc-3680-event-package threshold percentage <*value*>

Syntax Description

deregister-on-termination	Specifies that deregistration occurs when subscription terminates.
expire-time <*value*>	Specifies the expiration time, in seconds, for the RFC 3680 event package subscription. Valid range is **60** to **86400** seconds.
threshold	Specifies the threshold for RFC 3680 event package subscription expiration.
absolute <*value*>	Specifies the expiration threshold as an absolute value. Valid range is **5** to **604800** seconds, and must be less than the specified expiration time.
percentage <*value*>	Specifies the expiration threshold as a percentage. Valid range is **1** to **100** percent.

Default Values

By default, this feature is disabled.

Command History

Release R13.8.0	Command was introduced.

Usage Examples

The following example enables subscription to RFC 3680 event packages for successful registrations on SIP trunk T01, and specifies that the trunk is deregistered when the subscription terminates:

(config)**#voice trunk t01 type sip**
(config-t01)**#subscribe rfc-3680-event-package deregister-on-termination**

transfer-mode

Use the **transfer-mode** command to specify the behavior of the Session Initiation Protocol (SIP) trunk when configured in a network with a Netvanta Unified Communications product. This feature determines whether transferred calls will be controlled by the unit locally, or by the network. Use the **no** form of this command to return to the default setting. Variations of this command include:

transfer-mode local
transfer-mode network

Syntax Description

local	Specifies that call transferring is controlled locally by the unit.
network	Specifies that call transferring is controlled by the network.

Default Values

By default, the network controls call transfers.

Command History

Release A4.05	Command was introduced for the NetVanta 7000 Series products.

Functional Notes

When this command is issued on a specific SIP trunk, it overrides the **voice transfer-mode** configuration (if previously set in the Global Configuration mode) but only applies the new configuration setting to the SIP trunk on which it was issued. Refer to *voice transfer-mode on page 1975* for more information on using the Global command.

Usage Examples

The following example configures the network to handle call transfers:

(config)**#voice trunk t01 type sip**
(config-t01)**#transfer-mode network**

trunk-group-id *<label> <context>*

Use the **trunk-group-id** command to specify an RFC 4904 trunk group identifier in outbound SIP INVITEs on the specified trunk. Use the **no** form of this command to return to the default setting. Variations of this command include:

trunk-group-id *<label> <context>*
trunk-group-id *<label> <context>* **always**

Syntax Description

<label>	Specifies the label for the trunk group identifier. Valid entries consist of any alphanumeric characters with a maximum length of 20 characters.
<context>	Specifies the context for the trunk group identifier. Valid entries consist of any alphanumeric characters with a maximum length of 50 characters.
always	Optional. Specifies to add the trunk group identifier even if no caller ID information is present.

Default Values

By default, there no trunk group id is defined.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example specifies a trunk-group-id with the label **2565550100** and context **voip.example**:

(config)**#voice trunk t01 type sip**
(config-t01)**#trunk-group-id 2565550100 voip.example**

trust-domain

Use the **trust-domain** command to add security measures for users' identity and privacy by connecting the trunk to a trusted domain. Using the trusted domain adds another level of privacy from participating service providers. The system supports RFC 3323 and RFC 3325. Use the **no** form of this command to return to the default setting. Variations of this command include the following:

trust-domain
trust-domain p-asserted-identity-required

Syntax Description

p-asserted-identity-required	Requires the use of P-Asserted-Identity SIP privacy for this trusted domain.

Default Values

By default, the **trust-domain** is disabled.

Command History

Release 13.1	Command was introduced.

Usage Examples

The following example enables the **trust-domain**:

(config)**#voice trunk t01 type sip**
(config-t01)**#trust-domain**

update-supported

Use the **update-supported** command to enable support for the UPDATE message for calls on the trunk. UPDATE messages containing SDP will only be accepted for SIP to TDM calls. Use the **no** form of this command to return to the default setting. Variations of this command include:

update-supported
update-supported forward-no-sdp

Syntax Description

forward-no-sdp	Optional. Allows the forwarding of in-dialog UPDATE requests that do not contain SDP to the other trunk involved in a call.

Default Values

By default, this feature is disabled.

Command History

Release A5.01	Command was introduced.
Release R13.8.0	Command was expanded to include the f**orward-no-sdp** parameter.

Usage Examples

The following example enables support for UPDATE messages for calls on SIP trunk T01:

(config)**#voice trunk t01 type sip**
(config-t01)**#update-supported**

vm-diversion

Use the **vm-diversion** command to apply a Session Initiation Protocol (SIP) Diversion header to calls forwarded to the external voice mail server. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this feature is disabled.

Command History

Release A4.01	Command was introduced.

Usage Examples

The following example enables **vm-diversion**:

(config)**#voice trunk t01 type sip**
(config-t01)**#vm-diversion**

VOICE T1 TRUNK COMMAND SET

Voice T1 trunks are trunks that use T1 circuits and robbed-bit signaling (RBS) to connect communication devices to the outside world. The T1 RBS trunk can terminate a line from the service provider, or be a termination point acting as the network to a private branch exchange (PBX) or key system requiring a T1 circuit. The term T1 circuit is commonly used to identify a multiplexed 24-channel, 1.544 Mbps digital data circuit, providing communications between two facilities or from a local service provider. T1 refers to the transport of a DS1-formatted signal onto a copper, fiber, or wireless medium for deploying voice, data, or video conferencing services. T1 connections provide up to 24 DSO channels of 64kbps, and use the RBS scheme to pass call signaling status information.

RBS is the process where the least significant bit in the sixth and twelfth frame (of a superframe (SF) T1) and the sixteenth and twentieth frame (of an extended superframe (ESF) T1) is *robbed* for voice A, B, C, and D signaling bits. These signaling bits indicate on-hook or off-hook conditions, as well as other signaling states.

Before configuring a T1 voice trunk, the T1 interface must be configured. For more information on configuring the T1 interface, refer to the *T1 Interface Command Set on page 2463*. Once the T1 interface is configured, you must create a T1 trunk account in order to make and receive calls. When creating the T1 trunk account, it is important to make sure the T1 RBS settings (supervision, type, etc.) match the parameters set by your service providers.

There are six main types of T1 trunks supported by AOS. The first is a T1 trunk without RBS, the second is a T1 RBS trunk using feature group D (FGD), the third is a T1 RBS trunk using ground start (GS), the fourth is a T1 RBS trunk using loop start (LS), the fifth is a T1 RBS trunk using wink, and the sixth is a T1 RBS trunk using immediate supervision.

To create a T1 trunk account without RBS and enter the Trunk Account Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01
(config-t01)#
```

To create a T1 RBS trunk account using FGD and enter the Trunk Account Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type t1-rbs supervision fgd role user
(config-t01)#
```


To create a T1 RBS trunk account using GS and enter the Trunk Account Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type t1-rbs supervision ground-start role user
(config-t01)#
```

To create a T1 RBS trunk using LS and enter the Trunk Account Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type t1-rbs supervision loop-start role user
(config-t01)#
```

To create a T1 RBS trunk account using wink and enter the Trunk Account Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type t1-rbs supervision wink role [network | user]
(config-t01)#
```

To create a T1 RBS trunk using immediate supervision and enter the Trunk Account Configuration mode, enter the following command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#voice trunk t01 type t1-rbs supervision immediate role [network | user]
(config-t01)#
```

*Not all T1 Trunk commands apply to all T1 trunk types. Use the **?** command to display a list of valid commands.*

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

alc

Use the **alc** command to enable automatic level control (ALC). ALC reduces Realtime Transport Protocol (RTP) received signals that are out of specification to the predefined levels. It is not necessary to enable ALC on those networks that guarantee signal levels to be within specification. Use the **no** form of this command to disable this feature. Variations of this command include:

alc
alc level -16
alc level -17
alc level -18
alc level -19
alc level -20
alc level -21
alc level -22

Syntax Description

level -16	Optional. Specifies the ALC attenuation level is -16 dBm0.
level -17	Optional. Specifies the ALC attenuation level is -17 dBm0.
level -18	Optional. Specifies the ALC attenuation level is -18 dBm0.
level -19	Optional. Specifies the ALC attenuation level is -19 dBm0.
level -20	Optional. Specifies the ALC attenuation level is -20 dBm0.
level -21	Optional. Specifies the ALC attenuation level is -21 dBm0.
level -22	Optional. Specifies the ALC attenuation level is -22 dBm0.

Default Values

By default, ALC is disabled.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Line Interface.
Release A2	Command was added to the Media Gateway Control Protocol (MGCP) endpoint configuration.
Release A2.04	Command was expanded to include the **level** parameters.

Usage Examples

The following example activates the ALC on trunk **T01**:

(config)**#voice trunk t01 type t1-rbs supervision loop-start role user**
(config-t01)**#alc**

blind-dial

Use the **blind-dial** command to allow calls to be placed without the presence of dial tone. Use the **no** form of this command to disable blind dialing.

Syntax Description

No subcommands.

Default Values

By default, **blind-dial** is disabled.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example enables blind dialing:

```
(config)#voice trunk t01 type t1-rbs supervision loop-start role user
(config-t01)#blind-dial
```

busy all

Use the **busy all** command to set all level zero digital signals (DS0s) to busy so that no calls are allowed inbound or outbound. If any calls are active at the time this command is issued, the calls will stay active until either party terminates the call. Once terminated, the DS0s are busied out. Use the **no** form of this command to disable this feature. Variations of this command include:

busy all
busy all now

Syntax Description

now	Optional. Immediately terminates calls that are active at the time the command is issued.

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets all DS0s on trunk **T01** to busy and terminates calls that are active at the time the command is issued:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#busy all now**

busy t1 <*slot/port*> tdm-group <*number*>

Use the **busy t1 tdm-group** command to set a particular set of level zero digital signals (DS0s) (defined in a time division multiplexing (TDM) group) to busy so that no calls are allowed inbound or outbound the interface. If any calls are active at the time this command is issued, the calls will stay active until either party terminates the call. Once terminated, the DS0s are set to busy. Use the **no** form of this command to disable this feature. Variations of this command include:

busy t1 <*slot/port*> **tdm-group** <*number*>
busy t1 <*slot/port*> **tdm-group** <*number*> **now**

Syntax Description

<*slot/port*>	Specifies the slot/port for the T1.
<*number*>	Specifies the TDM group ID number.
now	Optional. Terminates calls that are active at the time the command is issued (for example, in the middle of a conversation).

Default Values

No default values are necessary for this command.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example sets DS0s in TDM group **2** to **busy** and terminates calls that are active when the command is issued:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#busy t1 0/1 tdm-group 2 now**

caller-id

Use the **caller-id** number command to interpret and pass caller identification (ID) on this trunk. This information usually displays the name, number, time, and date of the calling party. Use the **no** form of this command to cancel the setting.

Syntax Description

No subcommands.

Default Values

By default, caller ID is disabled.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables caller ID:

(config)**#voice trunk t01 type t1-rbs supervision fgd role user**
(config-t01)**#caller-id**

caller-id-override

Use the **caller-id-override** command to replace the calling party information for this trunk with a specific number. This command is used to conceal a user's name and number or to display a different name and number for internal or external caller ID. Use the **no** form of this command to cancel the setting. Variations of this command include:

caller-id-override emergency-outbound <*number*>
caller-id-override emergency-outbound match-substitute
caller-id-override name-inbound <*name*>
caller-id-override name-inbound <*name*> **if-unavailable**
caller-id-override number-inbound <*number*>
caller-id-override number-inbound <*number*> **if-no-cpn**
caller-id-override number-inbound <*number*> <*trunk id*>
caller-id-override privacy-outbound match-substitute

Syntax Description

emergency-outbound	Replaces the calling party number for outbound emergency calls.
<*number*>	Specifies the number to replace the calling party number for outbound emergency calls.
match-substitute	Specifies that the configured automatic number identification (ANI) match substitution is used for outbound emergency calls.
name-inbound <*name*>	Specifies the name to replace the calling party name for inbound calls.
if-unavailable	Specifies that the calling party name is replaced only if the calling party name is unavailable.
number-inbound <*number*>	Specifies the number to replace the calling party number for inbound calls.
<*trunk id*>	Optional. Specifies the trunk ID (**Txx**) for outbound calls.
if-no-cpn	Optional. Specifies that the calling party number is replaced only if the calling party number is unavailable.
privacy-outbound	Replaces the calling party number on anonymous outbound calls.
match-substitute	Specifies that the configured ANI match substitution is used for anonymous outbound calls.

Default Values

No default values are necessary for this command.

Command History

Release 10.1	Command was introduced.
Release 15.1	Command was expanded.
Release 16.1	Command was expanded to include the **if-no-cpn** parameter.
Release A4.01	Command was expanded to include the **match-substitute** parameter.
Release R11.8.0	Command was expanded to include the **privacy-outbound** parameter.

Usage Examples

The following example sets the caller ID override number on the trunk where the command is issued:

(config)**#voice trunk t01 type analog supervision loop-start**
(config-t01)**#caller-id-override number-inbound 555-8000**

codec-list *<name>*

Use the **codec-list** command to specify the coder-decoder (CODEC) list to be used by this account. This CODEC can be used for normal voice traffic or for Session Border Controller (SBC) transcoding. Use the **no** form of this command to remove the CODEC list from the account. Variations of this command include:

codec-list *<name>*
codec-list *<name>* **both**
codec-list *<name>* **in**
codec-list *<name>* **out**
codec-list any
codec-list any both
codec-list any in
codec-list any out

Syntax Description

<name>	Specifies the CODEC list to be used for this account.
any	Specifies that any possible CODEC is allowed on this account.
both	Optional. Specifies that the CODEC list is applied to both transmitted and received Session Description Protocol (SDP) transmissions.
in	Optional. Specifies that the CODEC list is applied to received SDP only.
out	Optional. Specifies that the CODEC list is applied to transmitted SDP only.

Default Values

By default, no CODEC lists are assigned.

Command History

Release R10.4.0	Command was introduced and replaced the **codec-group** command.

Functional Notes

The **codec-list** command applies a previously configured CODEC list to an interface, voice trunk, or voice account. These lists are lists of CODECs used by the interface, trunk, or account in call negotiation and are arranged in preferred order with the first listed CODEC being the most preferred.

CODEC lists are created using the **codec** command from the Voice CODEC List Configuration mode prompt. For more information about creating CODEC lists, refer to the *Voice CODEC List Command Set on page 4893***.**

In addition, CODEC lists can be used for the SBC transcoding feature. For more information about this feature, its uses, and its configuration, refer to the configuration guide *Configuring Transcoding in AOS*, available online at https://supportcommunity.adtran.com.

*Because you can choose to specify that any CODEC is used by a Session Initiation Protocol (SIP) endpoint with the **any** keyword, do not create a CODEC list with the name of **any**.*

Usage Examples

The following example applies the CODEC list **LIST1** to incoming SDP traffic on trunk **T01**:

(config)**#voice trunk t1-rbs supervision wink role network**
(config-t01)**#codec-list LIST1 in**

connect t1 <*slot/port*> tdm-group <*number*>

Use the **connect t1 tdm-group** command to specify the physical interfaces this trunk group will use for voice connections. Refer to *tdm-group <number> on page 2478* for more information on creating time division multiplexing (TDM) groups. Use the **no** form of this command to remove this association.

Syntax Description

<slot/port>	Specifies the slot/port for the T1.
<number>	Specifies the TDM group ID number.

Default Values

By default, no physical interface is assigned.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example specifies that this trunk will use the level zero digital signals (DS0s) in TDM group **3** (on T1 interface **0/1**):

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#connect t1 0/1 tdm-group 3**

dialtone

Use the **dialtone** command to enable dial tone generation. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the dial tone is enabled.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example disables dial tone on trunk **T01**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#no dialtone**

did digits-transferred

Use the **did digits-transferred** command to define how many of the received digits should be sent to the internal switchboard from an incoming call on a user role trunk. The number of digits transferred are the least significant digits received. Direct inward dialing (DID) should be used if a Telco provider is providing digits to the unit on inbound calls or if the unit needs to provide DID information to a piece of customer premises equipment (CPE). Use the **no** form of this command to disable this feature. Variations of this command include:

did digits-transferred <*value*>
did digits-transferred <*value*> **prefix** <*number*>

Syntax Description

<*value*>	Specifies the number of digits to be transferred. Range is **1** to **16** digits.
prefix <*number*>	Optional. Specifies a sequence of digits to be prepended to the digits that will be transmitted. For example, if seven digits will be transferred via DID, then prefix the seven digits with 256. Thus, **555-8000** would be prefixed with **256**, transmitting out the string of digits **256-555-8000**.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.

Functional Notes

User Role Example:

555-1000 is an incoming call on the trunk. With **did digits-transferred** <*value*> set to 4, the number 1000 will be sent to the switchboard. On a network role trunk, the **did digits-transferred** command allows you to define how many of the digits from the Accept criteria should be sent externally from a call that was routed by the switchboard. The number of digits transferred are the least significant digits received.

Network Role Example:

555-1000 is accepted on the universal time (UT) interface. With **did digits-transferred** <*value*> set to 4, the number of 1000 will be sent to the device connected to the UT interface. This command cannot be specified if and when **trunk-number** is being used. Conversely, if DID is used, **trunk-number** will not be allowed.

Usage Examples

The following example transfers the digits **555-8000** and adds the prefix **256**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#did digits-transferred 5558000 prefix 256**

dnis-digits <*value*> prefix <*number*>

Use the **dnis-digits prefix** command to program the number of digits to be transferred inbound on the specific trunk. Use the **no** form of this command to cancel the setting.

Syntax Description

<*value*>	Specifies the number of digits to be transferred.
<*number*>	Specifies the number prefix to prepend to the transferred digits.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example sets the number of transferred dialed number identification service (DNIS) digits to **4** on trunk **T01** and sets the prefix **555**:

(config)**#voice trunk t01 type t1-rbs supervision fgd role user**
(config-t01)**#dnis-digits 4 prefix 555**

early-cut-through

Use the **early-cut-through** command to provide the caller with inband ringback and other call progress signals. This command should not be issued if the connected equipment does not provide inband ringback and other call progress signals. This option is only valid for voice trunks in the network role. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **early-cut-through** is enabled.

Command History

Release A1	Command was introduced.

Usage Examples

The following example disables early-cut-through:

```
(config)#voice trunk t01 type t1-rbs supervision wink role network
(config-t01)#no early-cut-through
```

echo-cancellation

Use the **echo-cancellation** command to improve voice quality for packetized-based voice calls, such as Voice over Internet Protocol (VoIP) or Media Gateway Control Protocol (MGCP). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **echo-cancellation** is enabled.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example activates **echo-cancellation**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#echo-cancellation**

match ani <*template*> substitute <*template*>

Use the **match ani substitute** command to configure automatic number identification (ANI) substitution for outbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

match ani <*template*> **substitute** <*template*>
match ani <*template*> **substitute** <*template*> **name** <*name*>

Syntax Description

ani <*template*>	Specifies the ANI information to be substituted. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the ANI information that is substituted for the original ANI information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
name <*name*>	Optional. Specifies the name associated with the ANI information. This option is only available on trunks that support ANI name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no ANI substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for ANI templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the ANI information from numbers **555-8111** to **555-8115** will be substituted by **555-8110** for outbound calls on the trunk **T03**:

(config)**#voice trunk t03 type t1-rbs supervision wink role network**
(config-t03)**#match ani 555-811[125] substitute 555-8110**

match dnis <*template*> replace ani <*number*>

Use the **match dnis replace ani** command to replace dialed number identification service (DNIS) information with automatic number identification (ANI) information on outbound voice trunks. Use the **no** form of this command to remove the replacement. Variations of this command include:

match dnis <*template*> **replace ani** <*number*>
match dnis <*template*> **replace ani** <*number*> **name** <*name*>

Syntax Description

dnis <*template*>	Specifies the DNIS information to be replaced. This information is entered using wildcards and numerical digits. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
replace ani <*number*>	Specifies the ANI information that replaces the original DNIS information. This information is entered using numerical digits. Enter the number without punctuation.
name <*name*>	Optional. Specifies the name associated with the ANI information. This option is only available on trunks that support ANI name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no DNIS replacement is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for DNIS templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits

3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the DNIS information for dialed numbers on trunk **T03** that match **1-256-524-8600** are replaced with **882-6467**:

(config)**#voice trunk t03 type t1-rbs supervision wink role network**
(config-t03)**#match dnis 1-256-524-8600 replace ani 8826467**

match dnis <*template*> substitute <*template*>

Use the **match dnis substitute** command to configure dialed number identification service (DNIS) substitution for outbound voice trunks. Use the **no** form of this command to remove the substitution. Variations of this command include:

match dnis <*template*> **substitute** <*template*>
match dnis <*template*> **substitute** <*template*> **name** <*name*>

Syntax Description

dnis <*template*>	Specifies the DNIS information to be substituted. This information is entered using wildcards and numerical digits.Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
substitute <*template*>	Specifies the DNIS information that is substituted for the original DNIS information. This information is entered using wildcards and numerical digits. When using wildcards in the **match** and **substitute** template, both must be of the same type and position in the number template or AOS will not allow the substitution. Refer to the *Functional Notes* of this command for available wildcards and proper data entry.
name <*name*>	Optional. Specifies the name associated with the DNIS information. This option is only available on trunks that support DNIS name information (integrated services digital network (ISDN) trunks, Session Initiation Protocol (SIP) trunks, T1 loop start (LS) network trunks, and T1 ground start (GS) network trunks).

Default Values

By default, no DNIS substitution is configured.

Command History

Release A2	Command was introduced.

Functional Notes

The convention for DNIS templates is very similar to dial plan entries. Valid characters for templates are as follows:

0 - 9	Match the exact digit(s) only
X	Match any single digit 0 through 9
N	Match any single digit 2 through 9
M	Match any single digit 1 through 8
$	Match any number string dialed
[]	Match any digit in the list within the brackets (for example, [1,4,6])
,()	Formatting characters that are ignored but allowed
-	Use within brackets to specify a range, otherwise ignored

The following are example template entries using wildcards:

1) NXX-XXXX	Match any 7-digit number beginning with 2 through 9
2) 1-NXX-NXX-XXXX	Match any number with a leading 1, then 2 through 9, then any 2 digits, then 2 through 9, then any 6 digits
3) 555-XXXX	Match any 7-digit number beginning with 555
4) XXXX$	Match any number with at least 5 digits
5) [7,8]$	Match any number beginning with 7 or 8
6) 1234	Match exactly 1234

Some template number rules:

1) All brackets must be closed with no nesting of brackets and no wildcards within the brackets.
2) All brackets can hold digits and commas, for example: [1239]; [1,2,3,9]. Commas are implied between numbers within brackets and are ignored.
3) Brackets can contain a range of numbers using a hyphen, for example: [1-39]; [1-3,9].
4) The $ wildcard is only allowed at the end of the template, for example: 91256$; XXXX$.

Usage Examples

The following example specifies that the DNIS information for dialed numbers on trunk **T03** that match **1-334-NXX-XXXX** are substituted with **1-800-557-4500**:

(config)**#voice trunk t03 type t1-rbs supervision wink role network**
(config-t03)**#match dnis 1-334-NXX-XXXX substitute 1-800-557-4500**

modem-passthrough

Use the **modem-passthrough** command to switch to passthrough mode on fax or modem tone detection. This command allows modem and fax calls to maintain a connection without altering the signals with the voice improvement settings, such as echo cancellation and voice activity detection (VAD). Use the **no** form of this command to disable this feature. Variations of this command include:

modem-passthrough
modem-passthrough detection-time <*value*>
modem-passthrough cng-early-detect

Syntax Description

detection-time <*value*>	Optional. Specifies the fax and/or modem detection time length value in seconds. Range is **0** to **8** seconds.
cng-early-detect	Optional. Enables early (first burst) detection of fax calling (CNG) tone.

Default Values

By default, **modem-passthrough** is enabled.

Command History

Release 11.1	Command was introduced.
Release 12.1	Command was expanded.
Release R10.8.0	Command was expanded to include the **cng-early-detect** parameter.

Usage Examples

The following example disables **modem-passthrough**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#no modem-passthrough**

nls

Use the **nls** command to enable the non-linear suppression (NLS) option for the user. This option sets the echo canceller to reduce acoustic echo. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 14.1	Command was introduced.
Release 15.1	Command was added to the Voice Trunk T1 command set.

Usage Examples

The following example enables NLS on trunk **T01**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#nls**

plc

Use the **plc** command to enable packet loss concealment (PLC). PLC is used to prevent choppy connections by concealing a packet loss by replacing the lost packet with another voice packet in the data stream. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, PLC is enabled.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example disables PLC on trunk **T01**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#no plc**

prefer trunk-routing

Use the **prefer trunk-routing** command to add a trunk to a list of trunks that are considered first for call routing, regardless of system routing mode or locally configured extensions. Use the **no** form of this command to remove the trunk from the list.

Syntax Description

No subcommands.

Default Values

By default, **prefer trunk-routing** is disabled.

Command History

Release A2	Command was introduced.

Functional Notes

Trunk routing can be specified as a preference for specific trunks, allowing the trunk to be considered first for routing rather than relying on the internal or external nature of the call to dictate whether the trunk or voice station is the first choice routing path. The **prefer trunk-routing** command, executed from a specific trunk's configuration mode, adds the trunk to a list of trunks that are considered first for routing.

By default, no trunk routing preference is set, so that each trunk operates as dictated by normal call routing modes. Adding the trunk routing preference only affects how inbound calls from the specific trunk are handled.

Usage Examples

The following example specifies that trunk routing is preferred on the trunk **T01**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#prefer trunk-routing**

reject-external

Use the **reject-external** command to prevent inbound calls on the trunk from being routed back out of the same trunk. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, **reject-external** is enabled on this interface.

Command History

Release 9.3	Command was introduced.

Functional Notes

In general, trunks are assigned to the user role, which means they terminate lines from a Telco provider. If this is the case, **reject-external** should be enabled so that inbound calls on the trunk cannot be routed back out of the same trunk. If the configuration is poor, inbound long distance calls could be routed back out of the same trunk, causing the owner of the unit to be charged for long distance calls without his knowledge. For network-role trunks and Session Initiation Protocol (SIP) based trunks, this command should be disabled to allow calls to be properly routed in the unit.

Usage Examples

The following example disables **reject-external**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#no reject-external**

resource-selection

Use the **resource-selection** command to determine how the switchboard uses outbound call resources contained within a time division multiplexing (TDM) based trunk group. Use the **no** form of this command to disable this feature. Variations of this command include:

resource-selection circular
resource-selection circular ascending
resource-selection circular descending
resource-selection linear
resource-selection linear ascending
resource-selection linear descending

Syntax Description

circular	Performs call load balancing among available DS0s/B-channels in this trunk. Subsequent calls will be delivered to the next available DS0/B-channel in a round-robin fashion.
linear	Specifies that a call being delivered to this trunk will be accepted out the first available DS0/B-channel available at the time the call is received.
ascending	Optional. Distributes calls in an order from the lowest to the highest channel (DS0 1, 2, 3 through 24).
descending	Optional. Distributes calls in an order from the highest to the lowest channel (DS0 24, 23, 22 through 1).

Default Values

By default, resource selection is set to **linear**.

Command History

Release 9.3	Command was introduced.
Release 13.1	Command was expanded to include the **ascending** and **descending** subcommands.

Usage Examples

The following example specifies **circular** resource selection:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#resource-selection circular**

rtp delay-mode

Use the **rtp delay-mode** command to configure the Realtime Transport Protocol (RTP) jitter buffer packet delay mode settings. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Use the **no** form of this command to return to the default setting. Variations of this command include:

rtp delay-mode adaptive
rtp delay-mode fixed

Syntax Description

adaptive	Configures the RTP jitter buffer packet delay to adjust during a call based on network conditions.
fixed	Configures the RTP jitter buffer packet delay to remain constant.

Default Values

By default, the RTP delay mode is set to **adaptive**.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures RTP delay mode as **fixed**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#rtp delay-mode fixed**

rtp dtmf-relay

Use the **rtp dtmf-relay** command to configure the method by which Realtime Transport Protocol (RTP) dual tone multi-frequency (DTMF) events are relayed. The dial digits can be sent inband or out-of-band (OOB) of the voice stream. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp dtmf-relay inband
rtp dtmf-relay nte <*value*>

Syntax Description

inband	Specifies that RTP DTMF events be relayed inband in the RTP stream.
nte <*value*>	Specifies that RTP DTMF events be relayed OOB using named telephone event (NTE). Enter an NTE value between **96** and **127**.

Default Values

By default, the **rtp dtmf-relay** is set for **NTE 101**.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example configures RTP DTMF relay events for **inband**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#rtp dtmf-relay inband**

rtp frame-packetization <*value*>

Use the **rtp frame-packetization** command to configure the Realtime Transport Protocol (RTP) frame packetization time in milliseconds for individual trunks and users. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Configures the RTP frame packetization time value in milliseconds. Select from **10**, **20**, **30**, or **40** milliseconds.

Default Values

By default, the **rtp frame-packetization** time is set to **20** milliseconds on all trunks and users.

Command History

Release 9.3	Command was introduced.
Release R10.8.0	Command was expanded to include **40** milliseconds.

Usage Examples

The following example sets the frame packetization time for trunk **T01** to **10** milliseconds:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#rtp frame-packetization 10**

rtp packet-delay

Use the **rtp packet-delay** command to configure the maximum Realtime Transport Protocol (RTP) packet delays. This command is used to set the allowable limits of latency on the network. Use the **no** form of this command to return to the default value. Variations of this command include:

rtp packet-delay fax <*value*>
rtp packet-delay maximum <*value*>
rtp packet-delay nominal <*value*>

Syntax Description

fax <*value*>	Sets the fax delay time value. Range is **0** to **500** milliseconds.
maximum <*value*>	Sets the maximum delay time value in increments of **10** milliseconds. Range is **40** to **320** milliseconds.
nominal <*value*>	Sets the nominal delay time value in increments of **10** milliseconds. Range is **10** to **240** milliseconds.

Default Values

By default, the RTP packet delay for fax is **300**, maximum is **100**, and nominal is **50**.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the RTP fax delay time on trunk **T01** to **200** milliseconds:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#rtp packet-delay fax 200**

rtp qos dscp <*value*>

Use the **rtp qos dscp** command to configure the maximum Realtime Transport Protocol (RTP) quality of service (QoS) parameters for differentiated services code point (DSCP). Use the **no** form of this command to return to the default global value.

Syntax Description

<*value*>	Configures the RTP QoS parameter for DSCP. Enter a value between **0** and **63**.

Default Values

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. QoS is set using a DSCP value. The default global DSCP value for RTP is **46**.

Command History

Release 9.3	Command was introduced.

Functional Notes

By setting the **rtp qos dscp** value on an individual trunk or user, you will override the global **rtp qos dscp** setting for RTP packets. QoS is set using a DSCP value. Valid DSCP values are **0** to **63**, and a higher DSCP value has a higher priority. The default global DSCP value for RTP is **46**. Remember that if you are using a public IP connection, such as the Internet, for Voice over Internet Protocol (VoIP), end-to-end QoS may not be guaranteed. The default DSCP value for Session Initiation Protocol (SIP) is **26**. To configure QoS for the RTP traffic that carries the voice conversation, use the command **ip rtp qos dscp** followed by the desired DSCP value.

Usage Examples

The following example configures the RTP QoS DSCP for trunk **T01** to **60**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#rtp qos dscp 60**

rtp rx-gain *<value>*

Use the **rtp rx-gain** command to specify the Realtime Transport Protocol (RTP) receive (RX) gain or attenuation. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Using the **no** form of this command returns the RTP RX gain or attenuation to the default value.

Syntax Description

<value>	Specifies the RTP RX gain or attenuation in the RTP to time division multiplexing (TDM) direction. Range is **6** to **-14**. Negative values specify attenuation. Positive values specify gain in decibels (dB).

Default Values

By default, RTP RX gain is set to **0** dB.

Command History

Release A2.04	Command was introduced.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example specifies the RTP RX gain for trunk **T01** is **4** dB:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t01)**#rtp rx-gain 4**

rtp tx-gain *<value>*

Use the **rtp tx-gain** command to specify the Realtime Transport Protocol (RTP) transmit (TX) gain or attentuation. RTP is used to prevent static on voice connections by enhancing the quality of the packet delivery. Using the **no** form of this command returns the RTP TX gain or attenuation to the default value.

Syntax Description

<value>	Specifies the RTP TX gain or attenuation in the time division multiplexing (TDM) to RTP direction. Range is **6** to **-14**. Negative values specify attenuation. Positive values specify gain in decibels (dB).

Default Values

By default, RTP TX gain is set to **0** dB.

Command History

Release A2.04	Command was introduced.

Usage Examples

The following example specifies the RTP TX gain for trunk **T01** is **4** dB:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t01)**#rtp tx-gain 4**

treat-inbound-as-internal

Use the **treat-inbound-as-internal** command to make incoming trunk calls appear as internal calls. Use the **no** form of this command to cancel the setting.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.

Usage Examples

The following example configures the unit to treat inbound calls on trunk **T03** as internal calls:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#treat-inbound-as-internal**

trunk-number <*number*>

Use the **trunk-number** command to define the call routing when direct inward dialing (DID) is disabled. This feature directs incoming calls to the specified number when DID is not present. This command also allows users to activate different system modes of operation that redirect incoming calls to a different number depending on the specified mode. Use the **no** form of this command to disable this feature. Variations of this command include:

trunk-number <*number*>
trunk-number custom1 <*number*>
trunk-number custom1 no-number
trunk-number custom2 <*number*>
trunk-number custom2 no-number
trunk-number custom3 <*number*>
trunk-number custom3 no-number
trunk-number lunch <*number*>
trunk-number lunch no-number
trunk-number night <*number*>
trunk-number night no-number
trunk-number no-number
trunk-number override <*number*>
trunk-number override no-number
trunk-number weekend <*number*>
trunk-number weekend no-number

Syntax Description

<*number*>	Specifies the number used for call routing when DID is disabled.
custom1 - custom3	Specifies the custom mode to use.
lunch	Specifies the lunch-time mode.
night	Specifies the night-time mode.
no-number	Specifies no inbound calls are allowed on this trunk.
override	Specifies the override mode.
weekend	Specifies the weekend mode.

Default Values

No default values are necessary for this command.

Command History

Release 11.1	Command was introduced.
Release 15.1	Command was added to the feature group D (FGD) trunk options.
Release 16.1	Command was expanded to include the new subcommands.

Usage Examples

The following example defines call routing on trunk **T03**:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#trunk-number 4000**

t38

Use the **t38** command to enable T.38 fax operation. Use the **no** form of this command to disable this feature.

> NOTE *The **modem-passthrough** command must be enabled for T.38 operation to work. Refer to modem-passthrough on page 5176.*

Syntax Description

No subcommands.

Default Values

By default, T.38 is disabled.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables T.38 for trunk **T03**:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38**

Technology Review

T.38 is an International Telecommunication Union (ITU) specification that allows Group-3 Fax (T.30) data to be transported over the Internet. It is similar to dual tone multi-frequency (DTMF) relay (RFC 2833) in that the digital signal processor (DSP) decodes tones and demodulated fax data and converts them into packets. A similar device on the other end takes the packets/tones and remodulates them so that an analog fax machine on the other end can receive the fax. AOS's previous support (revisions 12 through 15) for fax/modem signals was simply detecting a tone and forcing the coder-decoder (CODEC) into G.711 and disabling/enabling echo cancellers based on the tones detected. When packet loss becomes high, sending faxes over G.711 becomes problematic, due to dropped messages and timeouts/retrains.

T.38 can be used in conjunction with various call-control schemes, such as H.323, Session Initiation Protocol (SIP), and Media Gateway Control Protocol (MGCP). AOS only supports SIP as the call-control method. This is typically referred to T.38/Annex-D. Annex-D describes the Session Initiation Protocol/Session Description Protocol (SIP/SDP) call establishment procedures.

t38 ced auto-generate

Use the **t38 ced auto-generate** command to specify when the digital signal processor (DSP) should regenerate the called station identifier (CED) signal toward the time division multiplexed (TDM) endpoint. If auto-generate is enabled, the DSP generates the CED signal only when it does not receive CED indicator packets from the Voice over IP (VoIP) endpoint. If auto-generate is disabled, the DSP generates the CED signal only when it does receive CED indicator packets from the VoIP endpoint. Using the **no** version of this command disables CED auto-generate.

Syntax Description

No subcommands.

Default Values

By default, CED auto-generate is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example enables CED auto-generate for the T.38 session on the trunk:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 ced auto-generate**

t38 ced length <*time*>

Use the **t38 ced length** command to set the maximum duration of a regenerated called station identifier (CED) signal, in milliseconds, from the digital signal processor (DSP) toward the time division multiplexed (TDM) endpoint when a T.38 session is active. Using the **no** form of this command returns the duration to the default value.

Syntax Description

<*time*>	Specifies the maximum duration of a regenerated CED signal in milliseconds. Valid range is **0** to **4000** ms.

Default Values

By default, the maximum duration of a regenerated CED signal is **3000** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Setting the maximum duration of a regenerated CED signal to **0** effectively prevents any CED generation.

Usage Examples

The following example decreases the maximum duration of the CED signal to **2000** ms for the T.38 session:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 ced length 2000**

t38 cng-relay-selective

Use the **t38 cng-relay-selective** command to enable fax calling tones (CNG) relay only when V.21 messages are not being transmitted. Use the **no** version of this command to disable selective CNG relay.

Syntax Description

No subcommands.

Default Values

Selective CNG relay is disabled by default.

Command History

Release R10.4.0	Command was introduced.

Usage Examples

The following example enables T.38 CNG relay:

(config)**#voice trunk t01 type t1-rbs supervision fgd role user**
(config-t03)**#t38 cng-relay-selective**

t38 ecm

Use the **t38 ecm** command to enable or disable error correction mode (ECM) during T.38 sessions. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 ecm enable
t38 ecm disable

Syntax Description

enable	Enables ECM during T.38 sessions.
disable	Disables ECM during T.38 sessions.

Default Values

By default, ECM is enabled.

Command History

Release R10.8.0	The command was introduced

Usage Examples

The following example disables ECM for T.38 sessions on trunk T03:

(config)**#voice trunk t01 type t1-rbs supervision fgd role user**
(config-t03)**#t38 ecm disable**

t38 error-correction

Use the **t38 error-correction** command to specify the type of fax error correction. Use the **no** form of this command to disable this feature. Variations of this command include:

t38 error-correction fec
t38 error-correction redundancy

Syntax Description

fec	Specifies forward error correction (FEC) as the fax error correction. FEC is a system of error control where the sender adds redundant data to its messages, allowing the receiver to detect and correct errors (within certain bounds) without the need to request additional data from the sender.
redundancy	Specifies redundancy as the fax error correction. Redundancy error correction replicates the payload a user-specified number of times to determine if errors are present. The number of redundant packets is set using the command *t38 v21-preamble-timeout <value> on page 5204*).

Default Values

By default, **t38 error-correction** is set to **redundancy** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, the NetVanta 6240/6250 Serires, and the NetVanta 640 Series.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default value changed to **fec** for the Total Access 900(e) Series, the NetVanta 6310/6330 Series, the NetVanta 6355 Series, and the NetVanta 7000 Series products.
Release R10.8.0	The default values for this command were updated.

Usage Examples

The following example sets the **t38 error-correction** to **fec**:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 error-correction fec**

t38 fallback-mode g711

Use the **t38 fallback-mode** command to specify the transmission mode used when T.38 fax relay cannot be successfully negotiated at the time of the fax transfer. Use the **no** form of this command to disable this feature.

Syntax Description

g711	Specifies that fax operation revert back to analog mode (G.711).

Default Values

By default, **t38 fallback-mode** is to **G.711**.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **G.711**.

Usage Examples

The following example enables the **t38 fallback-mode** on trunk **T02**:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 fallback-mode g711**

t38 generate-cng

Use the **t38 generate-cng** command to specify whether the digital signal processor (DSP) will begin a T.38 session by generating the calling signal (CNG) toward the time division multiplexed (TDM) endpoint. Using the **no** version of this command disables CNG generation.

Syntax Description

No subcommands.

Default Values

By default, CNG generation is disabled.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

With the introduction of this command, the CNG generation behavior of the T.38 session is now configurable. In AOS firmware prior to A5.01, this behavior was not configurable, but rather was set to always generate this signal.

Usage Examples

The following example enables CNG generation for the T.38 session:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 generate-cng**

t38 max-buffer <*value*>

Use the **t38 max-buffer** command to set the maximum buffer size for T.38 fax operation. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-buffer** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **800** bytes.

Default Values

By default, the maximum buffer size is set to **200**.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-buffer** to **100**:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 max-buffer 100**

t38 max-datagram <*value*>

Use the **t38 max-datagram** command to set the maximum datagram value in this unit. Use the **no** form of this command to return to the default value.

Syntax Description

<*value*>	Specifies the value of the **max-datagram** attribute in the Session Description Protocol (SDP) offer when the T.38 session is initiated. Range is **0** to **300** bytes.

Default Values

By default, the maximum datagram value is set to **72** bytes.

Command History

Release 16.1	Command was introduced.
Release A5.01	Command default was changed to **72** bytes.

Usage Examples

The following example sets the **t38 max-datagram** to **100**:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 max-datagram 100**

t38 max-rate

Use the **t38 max-rate** command to specify the fax maximum rate. The actual transmission rate could be lower than specified rate if the receiving end cannot support the maximum rate. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 max-rate 14400
t38 max-rate 12000
t38 max-rate 2400
t38 max-rate 4800
t38 max-rate 7200
t38 max-rate 9600

Syntax Description

14400	Specifies 14400 bits per second (bps) as fax maximum rate.
12000	Specifies 12000 bps as fax maximum rate.
2400	Specifies 2400 bps as fax maximum rate.
4800	Specifies 4800 bps as fax maximum rate.
7200	Specifies 7200 bps as fax maximum rate.
9600	Specifies 9600 bps as fax maximum rate.

Default Values

By default, the maximum fax rate is set to **14400** bps.

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example sets the **t38 max-rate** to **4800** bps:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 max-rate 4800**

t38 redundancy

Use the **t38 redundancy** command to set the number of redundant packets sent when the **t38 error-correction redundancy** feature is enabled. Use the **no** form of this command to return to the default value. Variations of this command include:

t38 redundancy high-speed <*value*>
t38 redundancy low-speed <*value*>

Syntax Description

high-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for data messages (high-speed fax machine image data). Range is **0** (no redundancy) to **4** packets.
low-speed <*value*>	Specifies the number of redundant T.38 fax packets to be sent for the signaling messages (low-speed fax machine protocol). Range is **0** (no redundancy) to **7** packets.

Default Values

By default, high-speed and low-speed redundancy values are set to **0** (no redundancy).

Command History

Release 16.1	Command was introduced.

Usage Examples

The following example enables **t38 error-correction redundancy** and sets the number of redundant data messages to **3** for trunk **T01**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#t38 error-correction redundancy**
(config-t01)**#t38 redundancy high-speed 3**

t38 v21-preamble-timeout *<value>*

Use the **t38 v21-preamble-timeout** command to set the maximum amount of time that the digital signal processor (DSP) waits for peer device activity after starting to transmit a V.21 preamble event before spoofing a response to the time division multiplexed (TDM) endpoint. Using the **no** version of this command returns the timeout value to the default setting.

Syntax Description

<value>	The time, in milliseconds, that the DSP will wait for peer activity. Valid range is **1** to **3000** ms.

Default Values

By default, the V.21 preamble timeout is set to **1700** ms.

Command History

Release A5.01	Command was introduced.

Functional Notes

This command is only available on AOS voice products that have Freescale DSP. This includes the Total Access 900(e) Series, the NetVanta 6310/6330 Series, and the NetVanta 7000 Series products.

This command is used to help in troubleshooting T.38 interoperability issues. This command should only be issued by advanced users or at the direction of Adtran technical support.

Usage Examples

The following example specifies the V.21 preamble timeout value as **2000** ms:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#t38 v21-preamble-timeout 2000**

tx-ani

Use the **tx-ani** command to transmit automatic number identification (ANI) (calling-party number) and dialed number identification service (DNIS) (called-party number) for outbound feature group D (FGD) calls. This command is only valid on a trunk configured for FGD supervision. Use the **no** form of this command to cancel the setting.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 12.1	Command was introduced.
Release 15.1	Command was added to the FGD command set.

Usage Examples

The following example configures the system to transmit ANI/DNIS information on the outbound FGD trunk:

(config)**#voice trunk t03 type t1-rbs supervision fgd role user**
(config-t03)**#tx-ani**

vad

Use the **vad** command to enable voice activity detection (VAD). VAD blocks out noise categorized as silence during a voice connection. The silent voice packets are not transmitted, allowing bandwidth usage to be reduced. Although VAD saves bandwidth, the quality of the voice call may be compromised. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, VAD is enabled for all T1 robbed-bit signaling (RBS) trunks and users.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example disables VAD on trunk **T01**:

(config)**#voice trunk t01 type t1-rbs supervision wink role network**
(config-t01)**#no vad**

VPN PARAMETER COMMAND SETS

The VPN parameter command sets are divided into the following sections:

CERTIFICATE COMMAND SETS

This section includes the following command sets:

CA PROFILE COMMAND SET

To activate the Certificate Authority (CA) Profile Configuration mode, enter the **crypto ca profile** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ca profile MyProfile
Configuring New CA Profile MyProfile
(ca-profile)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

crl optional on page 5210
email address <address> on page 5211
enrollment retry on page 5212
enrollment terminal on page 5213
enrollment url <url> on page 5214
fqdn <name> on page 5215
ip-address <ipv4 address> on page 5216
password <password> on page 5217
serial-number on page 5218
subject-name <name> on page 5219
uri <uri> on page 5220

crl optional

Use the **crl optional** command to make certificate revocation list (CRL) verification optional.

Syntax Description

No subcommands.

Default Values

By default, CRL optional is enabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

If enabled, AOS is able to accept certificates even if no CRL is loaded into the configuration. Currently, this is the only mode supported by AOS for CRL negotiations.

Usage Examples

The following example sets CRL verification as optional:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#crl optional**

email address <*address*>

Use the **email address** command to specify that an email address should be included in the certificate request. Use the **no** form of this command to remove an email address.

Syntax Description

<*address*>	Specifies the complete email address to use when sending certificate requests. This field allows up to 51 characters.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the email address only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <profile name> on page 1241*.

Usage Examples

The following example specifies **joesmith@company.com** as the email address to be sent in certificate requests:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#email address joesmith@company.com**

enrollment retry

Use the **enrollment retry** command to determine how AOS handles certificate requests. Use the **no** form of this command to return to the default setting. Variations of this command include:

enrollment retry count <*number*>
enrollment retry period <*value*>

Syntax Description

count <*number*>	Specifies the number of times AOS re-sends a certificate request when it does not receive a response from the previous request. Range is **1** to **100**.
period <*value*>	Specifies the time period between certificate request retries. The default is **1** minute between retries. Range is **1** to **60** minutes.

Default Values

By default, period is set to **5** minutes, and count is set to **12** retries.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures AOS to send certificate requests every **2** minutes, stopping after **50** retries (if no response is received):

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#enrollment retry count 50**
(ca-profile)**#enrollment retry period 2**

enrollment terminal

Use the **enrollment terminal** command to specify manual (i.e., cut-and-paste) certificate enrollment. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

This mode is overridden if the **enrollment url** command specifies the certificate authority (CA) to which automatic certificate requests are to be sent via Simple Certificate Exchange Protocol (SCEP). Issuing an **enrollment terminal** command after using the **enrollment url** command deletes the uniform resource locator (URL) and forces the unit to use manual enrollment. Refer to *enrollment url <url> on page 5214* for more information.

Usage Examples

The following example configures AOS to accept manual certificate enrollment input:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#enrollment terminal**

enrollment url <*url*>

Use the **enrollment url** command to specify the uniform resource locator (URL) of the certificate authority (CA) to which AOS should send certificate requests. Use the **no** form of this command to remove a URL.

Syntax Description

<*url*>	Specifies the certificate authority's URL (for example, **http://10.10.10.1:400/abcdefg/pkiclient.exe**).

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

When entering the URL, **http://** is required followed by the IP address or domain naming system (DNS) of the CA. If the port number is something other than 80, include it after the IP address or DNS name separated with a colon (**:**).

The CA may have other necessary information to include in the common gateway interface (CGI) path before ending with the actual CGI program. An example template to follow is **http://hostname:port/path/to/program.exe**.

Use the default program **pkiclient.exe** without specifying it, end the URL with a slash (**/**). Otherwise, you must enter the program name to use. For example, **http://10.10.10.1:400/abcdefg/** will assume **pkiclient.exe** as the program (but not including the terminating slash is a configuration error).

Specifying this command will override the **enrollment terminal** setting as described previously (refer to *enrollment terminal on page 5213*).

Usage Examples

The following example specifies **http://CAserver/certsrv/mscep/mscep.dll** as the URL to which AOS will send certificate requests:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#enrollment url http://CAserver/certsrv/mscep/mscep.dll**

fqdn *<name>*

Use the **fqdn** command to specify a fully qualified domain name (FQDN) to be included in the certificate requests. Use the **no** form of this command to remove an FQDN.

Syntax Description

<name>	Specifies the FQDN (e.g., **company.com**) to be included in requests.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the FQDN only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <profile name> on page 1241*.

Usage Examples

The following example specifies **company.com** as the FQDN to be sent in certificate requests:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#fqdn company.com**

ip-address *<ipv4 address>*

Use the **ip-address** command to specify an Internet Protocol version 4 (IPv4) address to be included in the certificate requests. Use the **no** form of this command to remove a defined IPv4 address.

Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the IPv4 address only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <profile name> on page 1241*.

Usage Examples

The following example specifies **66.203.52.193** as the IPv4 address to be sent in certificate requests:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#ip-address 66.203.52.193**

password *<password>*

Use the **password** command to specify the challenge password for Simple Certificate Exchange Protocol (SCEP). Use the **no** form of this command to allow certificate authority (CA) requests to be sent automatically (using SCEP) without requiring a password.

Syntax Description

<password>	Specifies the SCEP password (up to **80** characters).

Default Values

By default, no password is required.

Command History

Release 5.1	Command was introduced.

Functional Notes

There are two places for configuring a SCEP password:

- At the (ca-profile)# prompt.
- If it is not configured at the (ca-profile)# prompt, you are prompted to enter one when going through the certificate enrollment process.

The password is sent to the CA from which you are requesting a certificate. The CA may then ask for the password later before a certificate can be revoked. Refer to *crypto ca enroll <profile name> on page 1241*.

Usage Examples

The following example sets the SCEP challenge password to **adtran**:

(config)#**crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)#**password adtran**

serial-number

Use the **serial-number** command to specify that a serial number will be included in the certificate request. Use the **no** form of this command to prevent a serial number from being included in the certificate request.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Command History

Release 5.1	Command was introduced.

Functional Notes

By default, this command is set to **no serial-number**, which means that the serial number is not included in the certificate requests.

Usage Examples

The following example configures AOS to include a serial number in the certificate request:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#serial-number**

subject-name *<name>*

Use the **subject-name** command to specify the subject name used in the certificate request. Use the **no** form of this command to remove a configured subject name.

Syntax Description

<name>	Specifies a subject name string using up to **256** characters entered in X.500 Lightweight Directory Access Protocol (LDAP) format.

Default Values

By default, there is no subject name configured.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the subject name only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <profile name> on page 1241*.

Usage Examples

The following example assigns a subject name of **Adtran-cert** to certificate requests:

(config)**#crypto ca profile MyProfile**
Configuring New CA Profile MyProfile
(ca-profile)**#subject-name Adtran-cert**

uri *<uri>*

Use the **uri** command to configure a Uniform Resource Identifier (URI) value to be added to the certificate request at enrollment. The specified URI is included in the resulting certificate request and can be used for certificate validation. This option is useful when using features like SIPConnect. Use the **no** form of this command to remove the value from the certificate authority (CA) profile.

Syntax Description

<uri>	Specifies the URI in the format **x@y:port**.

Default Values

By default, no URI value is specified for the certificate.

Command History

Release R11.5.0	Command was introduced.

Functional Notes

Specifying the certificate URI is used in conjunction with the command *crypto ca enroll <profile name> on page 1241*.

Usage Examples

The following example configures a URI value to include in the certificate request:

(config)**#crypto ca enroll MYPROFILE**
(config-ca-profile-MYPROFILE)**#uri joesmith@example.com:5060**

CERTIFICATE COMMAND SET

To activate the Certificate Configuration mode, enter the **crypto ca certificate chain** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ca certificate chain MyProfile
(config-cert-chain)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

certificate <serial number> on page 5222
certificate ca <serial number> on page 5223
crl on page 5224

certificate *<serial number>*

Use the **certificate** command to restore a certificate. Use the **no** form of this command to remove a specific certificate from the certificate chain.

Syntax Description

<serial number>	Specifies the certificate's serial number (up to **51** characters). This value can be found for existing certificates by using the **show run** command.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

The user typically does not enter this command. It is primarily used to restore certificates from the startup configuration when the product is powered up.

Usage Examples

The following example removes the certificate with the serial number **73f0bfe5ed8391a54d1214390a36cee7**:

(config)**#crypto ca certificate chain MyProfile**
(config-cert-chain)**#no certificate 73f0bfe5ed8391a54d1214390a36cee7**

certificate ca *<serial number>*

Use the **certificate ca** command to restore a certificate authority (CA) certificate. Use the **no** form of this command to remove a specific certificate from the certificate chain for a CA.

Syntax Description

<serial number>	Specifies the certificate's serial number (up to **51** characters). This value can be found for existing certificates by using the **show run** command.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

The user typically does not enter this command. It is primarily used to restore certificates from the startup configuration when the product is powered up.

Usage Examples

The following example removes the CA certificate with the serial number **0712**:

(config)**#crypto ca certificate chain MyProfile**
(config-cert-chain)**#no certificate ca 0712**

crl

Use the **crl** command to restore a certificate revocation list (CRL). Use the **no** form of this command to remove the CRL for the specific certificate authority (CA).

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Command History

Release 5.1	Command was introduced.

Functional Notes

The user typically does not enter this command. It is primarily used to restore CRLs from the startup configuration when the product is powered up.

Usage Examples

The following example removes the CRL for the current CA:

(config)**#crypto ca certificate chain MyProfile**
(config-cert-chain)**#no crl**

CRYPTO MAP COMMAND SETS

This section includes the following command sets:

CRYPTO MAP IKE COMMAND SET

To activate the Crypto Map Internet Key Exchange (IKE) mode, enter a valid version of the **crypto map ipsec-ike** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto map MyMap 100 ipsec-ike
(config-crypto-map)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

antireplay on page 5227
commit-bit on page 5228
ike-policy <number> on page 5230
match address ip <ipv4 acl name> on page 5231
match track<name> on page 5233
reverse-route on page 5235
set peer on page 5237
set pfs on page 5239
set security-association idle-time <value> on page 5240
set security-association level per-host on page 5241
set security-association lifetime on page 5242
set transform-set on page 5243

For virtual private network (VPN) configuration example scripts, refer to the Virtual Private Network configuration guide available online at https://supportcommunity.adtran.com.

antireplay

Use the **antireplay** command to enable anti-replay sequence number checking for all security associations (SAs) created on this crypto map. Use the **no** form of this command to disable this feature. Variations of this command include:

antireplay
antireplay <*value*>

Syntax Description

<*value*>	Optional. Specifies the anti-replay window size in bytes. Select from **64**,**128**, **256**, **512**, or **1024** bytes.

Default Values

By default, the window size is set to **64** bytes.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables anti-replay sequence checking on crypto map **VPN 100**:

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#antireplay**

commit-bit

Use the **commit-bit** command to set the commit-bit in the Internet Security Association and Key Management Protocol (ISAKMP) header when sending the second message of quick mode on an IPsec tunnel negotiation. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the **commit-bit** will be used.

Command History

Release 12.1	Command was introduced.

Functional Notes

As an extra security measure, the commit-bit can be set by the responder of a quick mode negotiation to force the initiator to wait for the fourth message of quick mode before bringing up its IPsec security associations (SAs). By default, this feature is enabled on all AOS products with virtual private network (VPN) capabilities. Some vendors, however, may have incorrect implementations of the commit-bit that do not interoperate well with AOS products. In that case, the commit-bit should be disabled on all crypto maps that have a peer that does not support the commit-bit.

Usage Examples

The following example disables the use of commit-bit:

```
(config)#crypto map MyMap 100 ipsec-ike
(config-crypto-map)#no commit-bit
```

The following example displays a configuration with the commit-bit disabled:

```
ip crypto
!
crypto ike-policy 100
  initiate main
  respond main
  local-id address 10.10.10.1
  peer 192.168.1.1
  attribute 2
   encryption aes-256-cbc
   authentication pre-share
   lifetime 3600
!
```



```
crypto ike remote-id address 10.10.10.1 preshared-key adtran ike-policy 100 crypto map VPN 10
     no-mode-config no-xauth
!
crypto ipsec transform-set esp-aes-256-cbc-esp-sha-hmac esp-aes-256-cbc esp-sha-hmac mode tunnel
!
crypto map VPN 10 ipsec-ike
  description VPN to Main Site
  match address VPN-10-vpn-selectors
  set peer 192.168.1.1
  set transform-set esp-aes-256-cbc-esp-sha-hmac
  set security-association lifetime seconds 3600
  no commit-bit
  ike-policy 100
```

ike-policy *<number>*

Use the **ike-policy** command to ensure that only a specified Internet key exchange (IKE) policy is used to establish the IPsec tunnel. This prevents any mobile virtual private network (VPN) policies from using IPsec policies that are configured for static VPN peer policies. Use the **no** form of this command to remove a configured policy.

Syntax Description

<number>	Specifies the policy number of the policy to assign to this crypto map.

Default Values

No default values are necessary for this command.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sets the IKE policy **100** for crypto map **MyMap**:

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#ike-policy 100**

match address ip *<ipv4 acl name>*

Use the **match address ip** command to assign an Internet Protocol version 4 (IPv4) access control list (ACL) to a crypto map definition. The IPv4 ACL designates which IPv4 packets are to be encrypted by this crypto map. Use the **no** form of this command to delete an IPv4 ACL. Refer to *ip access-list extended <ipv4 acl name> on page 1344* for more information on creating ACLs.

Syntax Description

<ipv4 acl name>	Specifies the name of the IPv4 ACL you wish to assign to this crypto map.

Default Values

By default, no IPv4 ACLs are defined.

Command History

Release 4.1	Command was introduced.
Release R10.7.0	Command syntax was changed to require the **ip** keyword.

Functional Notes

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an IPv4 ACL. An IPv4 ACL is assigned to the crypto map using the **match address** command. If no IPv4 ACL is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

For a complete list of all extended ACL configuration commands, refer to the IPv4 Access Control List Command Set on page 4252.

The entries of the IPv4 ACL used in a crypto map should be created with respect to traffic sent by the Adtran product. The source information must be the local Adtran product and the destination must be the peer.

Only extended IPv4 ACLs can be used in crypto maps.

Usage Examples

The following example shows setting up an IPv4 ACL (called **NewList**) and then assigning the new list to a crypto map (called **NewMap**):

(config)**#ip access-list extended NewList**
(config-ext-nacl)**#exit**
(config)**#crypto map NewMap 10 ipsec-ike**
(config-crypto-map)**#match address ip NewList**

Technology Review

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of crypto map entries: **ipsec-manual** and **ipsec-ike**. Each entry is given an index, which is used to sort the ordered list.

When a nonsecured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the nonsecured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable security association (SA) exists, that is used for transmission. Otherwise, an SA is established based on the manual key configuration.

When a secured packet arrives on an interface, its security parameter index (SPI) is used to look up an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

match track<*name*>

Use the **match track** command to assign a network monitoring track to enable or disable the indicated crypto map policy. Use the **no** form of this command to remove this capability. Refer to *track <name> on page 1886* and *Network Monitor Track Command Set on page 4098* for more information on creating and using tracks.

Syntax Description

<name>	Specifies the name of the network monitoring track to assign to this crypto map.

Default Values

By default, there are no network monitoring tracks assigned.

Command History

Release 14.1	Command was introduced.

Functional Notes

To increase availability of a network with two virtual private network (VPN) gateways, a track can be assigned to a primary crypto map policy. This track will ensure connectivity to the primary VPN gateway. If the track detects connectivity problems on this gateway, the primary crypto map policy is disabled. Network traffic is then allowed to flow over the backup VPN gateway using the backup crypto map policy (which would have a similar **match address** access control list (ACL) as the primary crypto map policy). Once the track detects connectivity with the primary VPN gateway again, it will re-enable the primary crypto map policy.

Network monitoring tracks must be created first with the **track** command executed from the Global Configuration mode command prompt. Once created, further configuration is accomplished through the commands available in the *Network Monitor Track Command Set on page 4098*.

Usage Examples

The following example shows the preliminary steps necessary before assigning a track to a crypto map policy, as well as configuring the track to disable the primary VPN gateway if connectivity issues are detected.

Define a probe named **primaryping** to ping the primary VPN gateway (**10.22.156.251**):

```
(config)#probe primaryping icmp-echo
(config-probe-primaryping)#destination 10.22.156.251
(config-probe-primaryping)#period 10
(config-probe-primaryping)#tolerance consecutive fail 3
(config-probe-primaryping)#no shutdown
```

Create a track named **track1** to test the probe defined above:
(config)**#track track1**
(config-track-track1)**#test probe primaryping**
(config-track-track1)**#no shutdown**
(config-track-track1)**#exit**

Configure the crypto map (**NewMap**) to create a VPN tunnel to the primary VPN gateway (**10.22.156.251**):
(config)**#crypto map NewMap 10 ipsec-ike**
(config-crypto-map)**#description Primary VPN policy**
(config-crypto-map)**#match track track1**
(config-crypto-map)**#match address VPN-selectors**
(config-crypto-map)**#set peer 10.22.156.251**

Configure the crypto map (**NewMap**) to create a VPN tunnel to the backup VPN gateway (**10.22.156.240**):
(config)**#crypto map NewMap 20 ipsec-ike**
(config-crypto-map)**#description Backup VPN policy**
(config-crypto-map)**#match address VPN-selectors**
(config-crypto-map)**#set peer 10.22.156.240**

reverse-route

Use the **reverse-route** command to enable virtual private network (VPN) reverse route injection for a particular crypto map. Use the **no** form of this command to disable reverse route injection. Variations of this command include the following:

reverse-route
reverse-route <*number*>
reverse-route <*number*> **tag** <*value*>
reverse-route tag <*value*>

Syntax Description

<*number*>	Optional. Specifies the administrative distance for the static route. Range is **1** to **255**.
tag <*value*>	Optional. Specifies that a tag will be added to the static route in the route table. Range from **1** to **65535**.

Default Values

By default, reverse routing is disabled.

Command History

Release 15.1	Command was introduced.

Functional Notes

Reverse route injection automatically inserts a static route to a peer's remote network into the route table of a VPN gateway.

The tags used in reverse route injection allow the routes to be individuated from other static routes.

Usage Examples

The following example enables reverse route injection for crypto map **MyMap** with an administrative distance of **20** and a **tag** value of **10**:

(config)**#crypto map MyMap 100 ispec-ike**
(config-crypto-map)**#reverse-route 20 tag 10**

Technology Review

The reverse route injection allows a crypto IPsec policy to inject static routes to a remote network into its own route table, leaving it to the configuration of routing protocols to propagate the routes within the network. Reverse route injection serves as a method of updating routing tables when using a backup VPN server. In case one VPN is taken down or is unreachable, the VPN peer's route is removed out of the VPN gateway's route table and other route tables within the network.

Administrative distance is a feature that routers employ in order to select the most reliable path when there are two or more routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol by assigning a value (the smaller the value, the more trustworthy the protocol) that is then used by the router to organize routing protocols according to reliability.

set peer

Use the **set peer** command to set the IP address or host name of the peer device. Use the **no** form of this command to remove a peer device. Variations of this command include:

set peer <*ip address*>
set peer hostname <*hostname*>

Syntax Description

<*ip address*>	Specifies the IP address of the peer device. If this is not configured, it implies responder only to any peer. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
hostname <*hostname*>	Specifies the host name of the peer device expressed in the format <*host.example.com*> (for example, **vpn.somecompany.com**).

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release 16.1	Command was expanded to include the host name parameters.

Functional Notes

If no peer IP address or host name is configured, the entry will only be used to respond to IPsec requests; it cannot initiate the requests (since it doesn't know which IP address to which to send the packet). When a peer IP address is configured, the crypto map entry can be used to both initiate and respond to security associations (SAs). The peer address or host name is not checked when a tunnel is initiated from a remote unit; this address only serves as the virtual private network (VPN) peer to which to initiate a tunnel.

The peer IP address is the public IP address of the device that will terminate the IPsec tunnel. If the peer IP address is not static, or the peer’s address cannot be attained through the domain naming system (DNS) host name, the Adtran product cannot initiate the VPN tunnel. There are many Dynamic DNS services that can serve DNS for hosts that are dynamically addressed. By setting no peer IP address, the Adtran product can respond to an IPsec tunnel request.

Only one peer IP address or host name can be set.

When using DNS host names for peer IP addresses, the crypto map is not able to initiate a tunnel until the DNS host name resolves. This DNS host name is checked every 10 minutes.

Usage Examples

The following example sets the peer IP address of **10.100.23.64**:

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#set peer 10.100.23.64**

The following example sets the peer host name to **vpn.examplehost.com**:

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#set peer hostname vpn.examplehost.com**

set pfs

Use the **set pfs** command to choose the type of perfect forward secrecy (PFS), if any, that will be required during the IPsec negotiation of security associations (SAs) for this crypto map. Use the **no** form of this command to return to the default setting. Variations of this command include:

set pfs group1
set pfs group1 legacy-peer
set pfs group2
set pfs group2 legacy-peer
set pfs group5
set pfs group5 legacy-peer

Syntax Description

group1	Requires IPsec to use Diffie-Hellman Group 1 (768-bit modulus) exchange during IPsec security association (SA) key generation.
group2	Requires IPsec to use Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPsec SA key generation.
group5	Requires IPsec to use Diffie-Hellman Group 5 (1536-bit modulus) exchange during IPsec SA key generation.
legacy-peer	Optional. Specifies using the Diffie-Hellman secret generation for legacy peers (running AOS versions prior to A1.08 for voice products or 17.6.1 for data products).

Default Values

By default, no PFS will be used during IPsec SA key generation.

Command History

Release 4.1	Command was introduced.
Release 15.1	Command was expanded to include the **group5** parameter.
Release 17.6/A2.04	Command was expanded to include **legacy-peer** option.

Functional Notes

If left at the default setting, no PFS will be used during IPsec SA key generation. If PFS is specified, then the specified Diffie-Hellman Group exchange will be used for the initial and all subsequent key generation, thus providing no data linkage between prior keys and future keys.

Usage Examples

The following example specifies use of the Diffie-Hellman Group 1 exchange during IPsec SA key generation:

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#set pfs group1**

set security-association idle-time *<value>*

Use the **set security-association idle-time** command to set the receive idle timeout in seconds. This is the maximum amount of time for which the current virtual private network (VPN) peer can be idle. Once the timeout has occurred, the VPN tunnel will be brought down. Use the **no** form of this command to disable the timeout feature.

Syntax Description

<value>	Specifies the idle timeout in seconds. Valid range is **1** to **4294967294**.

Default Values

By default, the idle timeout is not defined.

Command History

Release 15.1	Command was introduced.

Usage Examples

The following example sets the receive idle timeout to **60** seconds:

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#set security-association idle-time 60**

set security-association level per-host

Use the **set security-association level per-host** command to enable per-host Internet Protocol (IP) security (IPsec) selector negotiation for the crypto map entry. When enabled, per-host mode specifies that the source and destination IP addresses of the packet requiring IPsec protection are placed in the virtual private network (VPN) selectors used in Quick Mode IPsec security association (SA) generation. Use the **no** form of this command to disable the per-host mode.

Exercise caution when enabling the per-host command. If many host-to-host conversations are being protected by the crypto map entry, a large number of IPsec SAs can be created, which can consume significant memory and processor resources on the device.

Syntax Description

No subcommands.

Default Values

By default, per-host mode is disabled.

Command History

Release R11.7.0	Command was introduced.

Functional Notes

Per-host mode applies only to crypto map entries keyed by Internet Key Exchange (IKE). This feature is not available in crypto maps keyed manually.

When per-host mode is enabled, and the device initiates Quick Mode, it replaces the source and destination networks in the crypto map entry access control list (ACL) line with the source and destination IP address of the packet requiring IPsec protection. Protocols and ports, if specified in the ACL, are negotiated as they are specified in the ACL line. This feature allows the hub in a Dynamic Multipoint VPN (DMVPN) network to select the appropriate outbound IPsec SA to protect traffic as it travels from the hub to a spoke.

The per-host setting does not apply when the device is responding to Quick Mode negotiations.

Usage Examples

The following example enables per-host mode on the crypto map:

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#set security-association level per-host**

set security-association lifetime

Use the **set security-association lifetime** command to define the lifetime (in kilobytes and/or seconds) of the IPsec security associations (SAs) created by this crypto map. Use the **no** form of this command to return to the default setting. Variations of this command include:

set security-association lifetime kilobytes <*value*>
set security-association lifetime seconds <*value*>

Syntax Description

kilobytes <*value*>	Specifies the SA lifetime limit in kilobytes.
seconds <*value*>	Specifies the SA lifetime limit in seconds.

Default Values

By default, the **security-association lifetime** is set to **28800** seconds, and there is no default for the kilobytes' lifetime.

Command History

Release 4.1	Command was introduced.

Functional Notes

Values can be entered for this command in both kilobytes and seconds. Whichever limit is reached first will end the SA.

Usage Examples

The following example sets the SA lifetime to **300** kilobytes and 2 hours (**7200** seconds):

(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#set security-association lifetime kilobytes 300**
(config-crypto-map)**#set security-association lifetime seconds 7200**

set transform-set

Use the **set transform-set** command to assign up to six transform sets to a crypto map. Use the **no** form of this command to return to the default setting. Refer to *data-call on page 1254* for information on defining transform sets. Variations of this command include:

set transform-set *<name>*
set transform-set *<name> <name>*
set transform-set *<name> <name> <name>*
set transform-set *<name> <name> <name> <name>*
set transform-set *<name> <name> <name> <name> <name>*
set transform-set *<name> <name> <name> <name> <name> <name>*

Syntax Description

<name>	Assigns up to six transform sets to this crypto map by listing the set names, separated by a space.

Default Values

By default, there is no transform set assigned to the crypto map.

Command History

Release 4.1	Command was introduced.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets that contain specific security algorithms (refer to *data-call on page 1254*).

If no transform set is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

Usage Examples

The following example first creates a transform set (**Set1**) consisting of two security algorithms (up to three may be defined), and then assigns the transform set to a crypto map (**MyMap**):

(config)**#crypto ipsec transform-set Set1 esp-3des esp-sha-hmac**
(cfg-crypto-trans)**#exit**
(config)**#crypto map MyMap 100 ipsec-ike**
(config-crypto-map)**#set transform-set Set1**

IPv4 Crypto Map Manual Command Set

To activate the Internet Protocol version 4 (IPv4) Crypto Map Manual mode, enter a valid version of the **ip crypto map ipsec-manual** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip crypto map Map-Name 10 ipsec-manual
(config-crypto-map)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

antireplay on page 5245
match address <name> on page 5246
set peer <ipv4 address> on page 5248
set session-key on page 5249
set transform-set <name> on page 5253

antireplay

Use the **antireplay** command to enable anti-replay sequence number checking for all security associations (SAs) created on this Internet Protocol version 4 (IPv4) crypto map. Use the **no** form of this command to disable this feature. Variations of this command include:

antireplay
antireplay <*value*>

Syntax Description

<*value*>	Optional. Specifies the anti-replay window size in bytes. Select from **64**, **128**, **256**, **512**, or **1024** bytes.

Default Values

By default, the window size is set to **64** bytes.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables anti-replay sequence checking on crypto map **VPN 100**:

(config)**#ip crypto map VPN 100 ipsec-manual**
(config-crypto-map)**#antireplay**

match address <*name*>

Use the **match address** command to assign an Internet Protocol version 4 (IPv4) access control list (ACL) to a crypto map definition. The IPv4 ACL designates the IPv4 packets to be encrypted by this crypto map. Use the **no** form of this command to remove a defined IPv4 ACL. Refer to *ip access-list extended <ipv4 acl name> on page 1344* for more information on creating ACLs.

Syntax Description

<name>	Specifies the name of the IPv4 ACL you wish to assign to this crypto map.

Default Values

By default, no IPv4 ACLs are defined.

Command History

Release 4.1	Command was introduced.

Functional Notes

IPv4 crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an ACL. An ACL is assigned to the crypto map using the **match address** command. If no ACL is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

For a complete list of all extended ACL configuration commands, refer to the *IPv4 Access Control List Command Set on page 4252*.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the Adtran product. The source information must be the local Adtran product, and the destination must be the peer.

Only extended ACLs can be used in crypto maps.

Usage Examples

The following example configures an IPv4 ACL (called **NewList**) and then assigning the new list to a crypto map (called **NewMap**):

(config)**#ip access-list extended NewList**

Configuring New Extended ACL "NewList"

(config-ext-nacl)**#exit**
(config)**#ip crypto map NewMap 10 ipsec-manual**
(config-crypto-map)**#match address NewList**

Technology Review

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of IPv4 crypto map entries: **ipsec-manual** and **ipsec-ike**. Each entry is given an index, which is used to sort the ordered list.

When a nonsecured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the nonsecured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable security association (SA) exists, that is used for transmission. Otherwise, an SA is established based on the manual key configuration.

When a secured packet arrives on an interface, its security parameter index (SPI) is used to look up an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

set peer *<ipv4 address>*

Use the **set peer** command to set the Internet Protocol version 4 (IPv4) address of the peer device. Use the **no** form of this command to remove a peer device.

Syntax Description

<ipv4 address>	Specifies the IPv4 address of the peer device. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.

Functional Notes

If no peer IPv4 address is configured, the manual crypto map is not valid and not complete. A peer IPv4 address is required for manual crypto maps. To change the peer IPv4 address, the **no set peer** command must be issued first; then the new peer IP address can be configured.

Usage Examples

The following example sets the peer IPv4 address of **10.100.23.64**:

(config)**#ip crypto map NewMap 10 ipsec-manual**
(config-crypto-map)**#set peer 10.100.23.64**

set session-key

Use the **set session-key** command to define the encryption and authentication keys for this Internet Protocol version 4 (IPv4) crypto map. Use the **no** form of this command to remove defined encryption and authentication keys. Variations of this command include the following:

set session-key inbound ah <*SPI*> <*key*>
set session-key inbound esp <*SPI*> **authenticator** <*key*>
set session-key inbound esp <*SPI*> **cipher** <*key*>
set session-key inbound esp <*SPI*> **cipher** <*key*> **authenticator** <*key*>
set session-key outbound ah <*SPI*> <*key*>
set session-key outbound esp <*SPI*> **authenticator** <*key*>
set session-key outbound esp <*SPI*> **cipher** <*key*>
set session-key outbound esp <*SPI*> **cipher** <*key*> **authenticator** <*key*>

Syntax Description

inbound	Defines encryption keys for inbound traffic.
outbound	Defines encryption keys for outbound traffic.
ah <*SPI*>	Specifies Authentication Header (AH) Protocol and security parameter index (SPI).
esp <*SPI*>	Specifies Encapsulating Security Payload (ESP) Protocol and SPI.
cipher <*key*>	Optional. Specifies encryption/decryption key.
authenticator <*key*>	Optional. Specifies authentication key.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.

Functional Notes

The inbound local SPI must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys.

Refer to the following list for key length requirements.

Algorithm:	Minimum key length required:
DES	64 bits in length; 8 hexadecimal bytes
3DES	192 bits in length; 24 hexadecimal bytes
AES-128-CBC	128 bits in length; 16 hexadecimal bytes
AES-192-CBC	192 bits in length; 24 hexadecimal bytes
AES-256-CBC	256 bits in length; 32 hexadecimal bytes
MD5	128 bits in length; 16 hexadecimal bytes
SHA1	160 bits in length; 20 hexadecimal bytes

Usage Examples

The following example configures an AOS product for virtual private network (VPN) using IPv4 IPSec manual keys. This example assumes that the AOS product has been configured with a wide area network (WAN) IPv4 address of **63.97.45.57** on interface **ppp 1** and a local area network (LAN) IPv4 address of **10.10.10.254** on interface **ethernet 0/1**. The peer private IPv4 subnet is **10.10.20.0**.

Step 1:
Enter the Global Configuration mode (i.e., config terminal mode).

>**enable**
#configure terminal

Step 2:
Enable VPN support using the **ip crypto** command. This command allows crypto maps to be applied to interfaces, and enables the Internet key exchange (IKE) server to listen for IKE negotiation sessions on User Datagram Protocol (UDP) port 500.

(config)**#ip crypto**

Step 3:
Define the transform set. A transform set defines the encryption and/or authentication algorithms to be used to secure the data transmitted over the VPN tunnel. Multiple transform sets may be defined in a system. Once a transform set is defined, many different crypto maps within the system can reference it. In this example, a transform set named **highly_secure** has been created. This transform set defines ESP with authentication implemented using 3DES encryption and SHA1 authentication.

(config)**#ip crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac**
(cfg-crypto-trans)**#mode tunnel**

Step 4:
Define an IP access control list (ACL). An extended ACL is used to specify which traffic needs to be sent securely over the VPN tunnel. The entries in the list are defined with respect to the local system. The source IP address will be the source of the traffic to be encrypted. The destination IP address will be the receiver of the data on the other side of the VPN tunnel.

(config)**#ip access-list extended corporate_traffic**
(config-ext-nacl)**#permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255 log**
deny ip any any

Step 5:
Create crypto map and define manual keys. A crypto map is used to define a set of encryption schemes to be used for a given interface. A crypto map entry has a unique index within the crypto map set. The crypto map entry will specify whether IKE is used to generate encryption keys, or if manually specified keys will be used. The crypto map entry will also specify who will be terminating the VPN tunnel, as well as which transform set or sets will be used to encrypt and/or authenticate the traffic on that VPN tunnel. It also specifies the lifetime of all created IPSec security associations (SAs).

The keys for the algorithms defined in the transform set associated with the crypto map will be defined by using the **set session-key** command. A separate key is needed for both inbound and outbound traffic. The key format consists of a string of hexadecimal values without the leading **0x** for each character. For example, a cipher key of **this is my cipher key** would be entered as:

7468697320697320D7920636970686572206B6579.

A unique SPI is needed for both inbound and outbound traffic. The local system's inbound SPI and keys will be the peer's outbound SPI and keys. The local system's outbound SPI and keys will be the peer's inbound SPI and keys. In this example, the following keys and SPIs are used:

Inbound cipher SPI: 300 Inbound cipher key: "2te$#g89jnr(j!@4rvnfhg5e"

Outbound cipher SPI: 400 Outbound cipher key: "8564hgjelrign*&(gnb#1$d3"

Inbound authenticator key:"r5%^ughembkdhj34$x.<"

Outbound authenticator key:"io78*7gner#4(mgnsd!3"

(config)**#ip crypto map corporate_vpn 1 ipsec-ike**
(config-crypto-map)**#match address corporate_traffic**
(config-crypto-map)**#set peer 63.105.15.129**
(config-crypto-map)**#set transform-set highly_secure**
(config-crypto-map)**#set session-key inbound esp 300 cipher**
32746524236738396A6E72286A21403472766E6668673565 authenticator
7235255E756768656D626B64686A333424782E3C
(config-crypto-map)**#set session-key outbound esp 400 cipher**
3835363468676A656C7269676E2A2628676E622331246433 authenticator
696F37382A37676E65722334286D676E73642133

Step 6:
Configure public interface. This process includes configuring the IPv4 address for the interface and applying the appropriate crypto map to the interface. Crypto maps are applied to the interface on which encrypted traffic will be transmitted.

(config)**#interface ppp 1**
(config-ppp 1)**#ip address 63.97.45.57 255.255.255.248**
(config-ppp 1)**#ip crypto map corporate_vpn**
(config-ppp 1)**#no shutdown**

Step 7:
Configure private interface to allow all traffic destined for the VPN tunnel to be routed to the appropriate gateway.

(config)**#interface ethernet 0/1**
(config-eth 0/1)**#ip address 10.10.10.254 255.255.255.0**
(config-eth 0/1)**#no shutdown**
(config-eth 0/1)**#exit**

set transform-set *<name>*

Use the **set transform-set** command to assign a transform set to an Internet Protocol version 4 (IPv4) crypto map. Use the **no** form of this command to remove assigned transform sets. Refer to *ip crypto ipsec transform-set <name> <parameters> on page 1352* for information on defining transform sets.

Syntax Description

<name>	Assigns a transform set to this crypto map by entering the set name.

Default Values

By default, no transform set is assigned to the crypto map.

Command History

Release 4.1	Command was introduced.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets that contain specific security algorithms (refer to *ip crypto ipsec transform-set <name> <parameters> on page 1352*).

If no transform set is configured for a crypto map, then the entry is incomplete and will have no effect on the system. For manual key crypto maps, only one transform set can be specified.

Usage Examples

The following example first creates a transform set (**Set1**) consisting of two security algorithms (up to three may be defined), and then assigns the transform set to a crypto map (**Map1**):

(config)**#ip crypto ipsec transform-set Set1 esp-3des esp-sha-hmac**
(cfg-crypto-trans)**#exit**

(config)**#ip crypto map Map1 1 ipsec-manual**
(config-crypto-map)**#set transform-set Set1**

IPV6 CRYPTO MAP MANUAL COMMAND SET

To activate the Internet Protocol version 6 (IPv6) Crypto Map Manual mode, enter a valid version of the **ipv6 crypto map ipsec-manual** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ipv6 crypto map Map-Name 10 ipsec-manual
(config-crypto6-map)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
description <text> on page 80
do on page 81
end on page 82
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

match address ipv6 <name> on page 5255
set peer <ipv6 address> on page 5256
set session-key on page 5257
set transform-set <name> on page 5259

match address ipv6 <*name*>

Use the **match address ipv6** command to assign an Internet Protocol version 6 (IPv6) access control list (ACL) to a crypto map definition. The IPv6 ACL designates the IPv6 packets to be encrypted by this crypto map. Use the **no** form of this command to remove a defined IPv6 ACL. Refer to *ipv6 access-list extended <ipv6 acl name> on page 1500* for more information on creating ACLs.

Syntax Description

<name>	Specifies the name of the IPv6 ACL you wish to assign to this crypto map.

Default Values

By default, no IPv6 ACLs are defined.

Command History

Release 4.1	Command was introduced.
Release 10.7.0	Command was expanded to include the **ipv6** keyword and IPv6 support.

Functional Notes

IPv6 crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an IPv6 ACL. An ACL is assigned to the crypto map using the **match address** command. If no ACL is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

For a complete list of all extended ACL configuration commands, refer to the IPv6 Access Control List Command Set on page 4296.

The entries of the IPv6 ACL used in a crypto map should be created with respect to traffic sent by the Adtran product. The source information must be the local Adtran product, and the destination must be the peer.

Only extended IPv6 ACLs can be used in crypto maps.

Usage Examples

The following example creates the IPv6 ACL (**NewList**) and applies it to the IPv6 crypto map **NewMap**:

(config)**#ipv6 access-list extended NewList**
(config-ext6-nacl)**#exit**
(config)**#ipv6 crypto map NewMap 10 ipsec-manual**
(config-crypto6-map)**#match address NewList**

set peer *<ipv6 address>*

Use the **set peer** command to set the Internet Protocol version 6 (IPv6) address of the peer device. Use the **no** form of this command to remove a peer device.

Syntax Description

<ipv6 address>	Specifies the IPv6 address of the peer device. IPv6 addresses should be expressed in colon hexadecimal format **X:X:X:X::X**, for example, **2001:DB8:1::1**.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release R10.7.0	Command was expanded to include IPv6 support.

Functional Notes

If no peer IPv6 address is configured, the manual crypto map is not complete and not valid. A peer IPv6 address is required for manual crypto maps. To change the peer IPv6 address, the **no set peer** command must be issued first; then the new peer IPv6 address can be configured.

If the peer address is link-local, the interface is assumed to be the interface having the crypto map assigned, and is the destination to which the protected packet is routed.

Usage Examples

The following example creates a peer on the crypto map to use for IPsec tunneling:

(config)**#ipv6 crypto map MAP1 10 ipsec-manual**
(config-crypto6-map)**#set peer 2001:DB8:1::1**

set session-key

Use the **set session-key** command to define the encryption and authentication keys for this Internet Protocol version 6 (IPv6) crypto map. Use the **no** form of this command to remove defined encryption and authentication keys. Variations of this command include the following:

set session-key inbound ah <*SPI*> <*key*>
set session-key inbound esp <*SPI*> **authenticator** <*key*>
set session-key inbound esp <*SPI*> **cipher** <*key*>
set session-key inbound esp <*SPI*> **cipher** <*key*> **authenticator** <*key*>
set session-key outbound ah <*SPI*> <*key*>
set session-key outbound esp <*SPI*> **authenticator** <*key*>
set session-key outbound esp <*SPI*> **cipher** <*key*>
set session-key outbound esp <*SPI*> **cipher** <*key*> **authenticator** <*key*>

Syntax Description

inbound	Defines encryption keys for inbound traffic.
outbound	Defines encryption keys for outbound traffic.
ah <*SPI*>	Specifies Authentication Header (AH) Protocol and security parameter index (SPI). Valid SPI range is **256** to **4294967295**.
esp <*SPI*>	Specifies Encapsulating Security Payload (ESP) Protocol and SPI. Valid SPI range is **256** to **4294967295**.
cipher <*key*>	Optional. Specifies encryption/decryption key. Keys are specified in hexadecimal format without the leading **0x**.
authenticator <*key*>	Optional. Specifies authentication key. Keys are specified in hexadecimal format without the leading **0x**.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.
Release R10.7.0	Command was expanded to include IPv6 support.

Functional Notes

The inbound local SPI must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys.

Refer to the following list for key length requirements.

Algorithm:	Minimum key length required:
DES	64 bits in length; 8 hexadecimal bytes
3DES	192 bits in length; 24 hexadecimal bytes
AES-128-CBC	128 bits in length; 16 hexadecimal bytes
AES-192-CBC	192 bits in length; 24 hexadecimal bytes
AES-256-CBC	256 bits in length; 32 hexadecimal bytes
MD5	128 bits in length; 16 hexadecimal bytes
SHA1	160 bits in length; 20 hexadecimal bytes

Both the inbound and outbound keys must be set for the crypto map.

Usage Examples

The following example defines the inbound and outbound authentication and encryption keys for the IPv6 crypto map **MAP1**:

(config)**#ipv6 crypto map MAP1 10 ipsec-manual**
(config-crypto6-map)**#set session-key inbound esp 300 cipher**
32746524236738396A6E72286A21403472766E6668673565 authenticator
7235255E756768656D626B64686A333424782E3C
(config-crypto6-map)**#set session-key outbound esp 400 cipher**
3835363468676A656C7269676E2A2628676E622331246433 authenticator
696F37382A37676E65722334286D676E73642133

set transform-set *<name>*

Use the **set transform-set** command to assign a transform set to an Internet Protocol version 6 (IPv6) crypto map. Use the **no** form of this command to remove assigned transform sets. Refer to *ipv6 crypto ipsec transform-set <name> <parameters> on page 1505* for information on defining transform sets.

Syntax Description

<name>	Assigns a transform set to this crypto map by entering the set name.

Default Values

By default, no transform set is assigned to the crypto map.

Command History

Release 4.1	Command was introduced.
Release R10.7.0	Command was expanded to include IPv6 support.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets that contain specific security algorithms (refer to *data-call on page 1254*).

If no transform set is configured for a crypto map, then the entry is incomplete and will have no effect on the system. For manual key crypto maps, only one transform set can be specified.

Usage Examples

The following example assigns the transform set **SET1** to crypto map **MAP1**:

(config)**#ipv6 crypto map MAP1 1 ipsec-manual**
(config-crypto6-map)**#set transform-set SET1**

IPSEC PROFILE COMMAND SET

The Internet Protocol Security (IPsec) Profile command set is used to configure a crypto IPsec profile to use in Dynamic Multipoint Virtual Private Network (DMVPN) configurations. This profile is used to simplify the configuration of VPN tunnels in a spoke-to-spoke or partial mesh DMVPN network by eliminating the need to define a crypto map entry and access control list (ACL) for each peer, as well as the traffic selectors in the ACLs for each remote or local network combination that requires IPsec protection. Instead, the profile provides protection to traffic traversing a tunnel interface by inferring a VPN peer address from the tunnel destination, the traffic selectors from the tunnel type, and the source and destination addresses of the tunnel interface. Once these parameters are known by the profile, protection is granted to traffic routed through the tunnel interface with the IPsec profile applied.

To activate the IPsec Profile Configuration mode, enter the **ip crypto ipsec profile** <*name*> command from the Global Configuration mode prompt as follows:

```
>enable
#configure terminal
(config)#ip crypto ipsec profile PROFILE1
(config-crypto-profile)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

description <text> on page 80
do on page 81
end on page 82
exit on page 83

All other commands for this command set are described in this section in alphabetical order.

antireplay <value> on page 5261
commit-bit on page 5262
ike-policy <number> on page 5263
rpf-check on page 5264
set pfs on page 5265
set security-association idle-time <value> on page 5266
set security-association lifetime on page 5267
set transform-set on page 5268

antireplay <*value*>

Use the **antireplay** command to enable anti-replay sequence number checking for all security associations (SAs) using this profile. Use the **no** form of this command to disable this feature. Variations of this command include:

antireplay
antireplay <*value*>

Syntax Description

<*value*>	Optional. Specifies the anti-replay window size in bytes. Select from **64**,**128**, **256**, **512**, or **1024** bytes.

Default Values

By default, the window size is set to **64** bytes.

Command History

Release 7.1	Command was introduced.
Release R11.9.0	Command was added to the IPsec Profile command set.

Functional Notes

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example enables anti-replay sequence checking for SAs using IPsec profile **PROFILE1** and sets the window size to **128** bytes:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#antireplay 128**

commit-bit

Use the **commit-bit** command to set the commit-bit in the Internet Security Association and Key Management Protocol (ISAKMP) header when sending the second message of quick mode on an IPsec tunnel negotiation. This feature verifies that encrypted payloads are not received until an SA is completely established. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, the **commit-bit** will be used.

Command History

Release 12.1	Command was introduced.
Release R11.9.0	Command was added to the IPsec Profile command set.

Functional Notes

As an extra security measure, the commit-bit can be set by the responder of a quick mode negotiation to force the initiator to wait for the fourth message of quick mode before bringing up its IPsec security associations (SAs). By default, this feature is enabled on all AOS products with virtual private network (VPN) capabilities.

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example disables the use of commit-bit on the SAs associated with IPsec profile **PROFILE1**:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#no commit-bit**

ike-policy *<number>*

Use the **ike-policy** command to ensure that only a specified Internet key exchange (IKE) policy is used to establish the IPsec tunnel for this profile. This prevents any mobile virtual private network (VPN) policies from using IPsec policies that are configured for static VPN peer policies. Use the **no** form of this command to remove a configured policy.

Syntax Description

<number>	Specifies the policy number of the policy to assign to this IPsec profile. Valid range is **1** to **10000**.

Default Values

By default, the IPsec profile is not assigned a specific IKE policy.

Command History

Release 6.1	Command was introduced.
Release R11.9.0	Command was added to the IPsec Profile command set.

Functional Notes

If an IKE policy is removed, references to that IKE policy in the IPsec profile must be removed manually to prevent an invalid configuration.

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example specifies that IPsec profile **PROFILE1** must use the IKE policy **100** to establish a tunnel:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#ike-policy 100**

rpf-check

Use the **rpf-check** command to enable reverse path forward (RPF) checking on the IPsec profile. This check refuses traffic on the tunnel if the tunnel's source and destination indicate the source of the traffic can be reached through a different tunnel or interface. Use the **no** form of this command to disable RFP checking on the profile.

Syntax Description

No subcommands.

Default Values

By default, RPF checking is enabled on the profile.

Command History

Release R11.9.0	Command was introduced.

Functional Notes

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example disables RPF checking on the IPsec profile **PROFILE1**:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#no rpf-check**

set pfs

Use the **set pfs** command to choose the type of perfect forward secrecy (PFS), if any, that will be required during the IPsec negotiation of security associations (SAs) for this IPsec profile. Use the **no** form of this command to return to the default setting. Variations of this command include:

set pfs group1
set pfs group2
set pfs group5

Syntax Description

group1	Requires IPsec to use Diffie-Hellman Group 1 (768-bit modulus) exchange during IPsec security association (SA) key generation.
group2	Requires IPsec to use Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPsec SA key generation.
group5	Requires IPsec to use Diffie-Hellman Group 5 (1536-bit modulus) exchange during IPsec SA key generation.

Default Values

By default, no PFS will be used during IPsec SA key generation.

Command History

Release 4.1	Command was introduced.
Release 15.1	Command was expanded to include the **group5** parameter.
Release 17.6/A2.04	Command was expanded to include **legacy-peer** option.
Release R11.9.0	Command was added to the IPsec Profile command set. This command set does not support the **legacy-peer** option.

Functional Notes

If left at the default setting, no PFS will be used during IPsec SA key generation. If PFS is specified, then the specified Diffie-Hellman Group exchange will be used for the initial and all subsequent key generation, thus providing no data linkage between prior keys and future keys.

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example specifies use of the Diffie-Hellman Group 1 exchange during IPsec SA key generation on the profile:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#set pfs group1**

set security-association idle-time *<value>*

Use the **set security-association idle-time** command to set the receive idle timeout in seconds. This is the maximum amount of time for which a security association (SA) pair associated with this IPsec profile can be idle. Once the timeout has occurred, the SA pair is removed. Use the **no** form of this command to disable the timeout feature.

Syntax Description

<value>	Specifies the idle timeout in seconds. Valid range is **20** to **1209600**.

Default Values

By default, the idle timeout is disabled.

Command History

Release 15.1	Command was introduced.
Release R11.9.0	Command was added to the IPsec Profile command set.

Functional Notes

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example sets the receive idle timeout for SA pairs associated with this profile to **60** seconds:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#set security-association idle-time 60**

set security-association lifetime

Use the **set security-association lifetime** command to define the lifetime (in kilobytes and/or seconds) of the IPsec security associations (SAs) associated to this IPsec profile. Use the **no** form of this command to return to the default setting. Variations of this command include:

set security-association lifetime kilobytes <*value*>
set security-association lifetime seconds <*value*>

Syntax Description

kilobytes <*value*>	Specifies the SA lifetime limit in kilobytes. Valid range is **2560** to **536870911** kilobytes.
seconds <*value*>	Specifies the SA lifetime limit in seconds. Valid range is **120** to **1209600** seconds.

Default Values

By default, the **security-association lifetime** is set to **28800** seconds.

Command History

Release 4.1	Command was introduced.
Release R11.9.0	Command was added to the IPsec Profile command set.

Functional Notes

Values can be entered for this command in both kilobytes and seconds. Whichever limit is reached first will end the SA.

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example sets the SA lifetime to **300** kilobytes and 2 hours (**7200** seconds) for SAs associated with IPsec profile **PROFILE1**:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#set security-association lifetime kilobytes 300**
(config-crypto-profile)**#set security-association lifetime seconds 7200**

set transform-set

Use the **set transform-set** command to assign up to six transform sets to the IPsec profile. Use the **no** form of this command to return to the default setting. Variations of this command include:

set transform-set *<name>*
set transform-set *<name> <name>*
set transform-set *<name> <name> <name>*
set transform-set *<name> <name> <name> <name>*
set transform-set *<name> <name> <name> <name> <name>*
set transform-set *<name> <name> <name> <name> <name> <name>*

Syntax Description

<name>	Assigns up to six transform sets to this IPsec profile by listing the set names, separated by a space.

Default Values

By default, there is no transform set assigned to the IPsec profile.

Command History

Release 4.1	Command was introduced.
Release R11.9.0	Command was added to the IPsec Profile command set.

Functional Notes

IPsec profiles do not directly contain the transform configuration for securing data. Instead, the profile is associated with transform sets that contain specific security algorithms (refer to the command *ip crypto ipsec transform-set <name> <parameters> on page 1352* for information about configuring transform sets). The parameters defined in one or more of the transform sets' peer(s) must match.

If no transform set is configured for an IPsec profile, then the profile is incomplete and will not function. This setting is required for an IPsec profile to operate.

When this setting is modified, all IPsec SAs created from this IPsec profile are deleted and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

Usage Examples

The following example assigns the transform set **SET1** to the IPsec profile **PROFILE1**:

(config)**#ip crypto ipsec profile PROFILE1**
(config-crypto-profile)**#set transform-set SET1**

IKE COMMAND SETS

This section includes the following command sets:

IKE CLIENT COMMAND SET

To activate the Internet Key Exchange (IKE) Client mode, enter the **crypto ike client** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ike client configuration pool ConfigPool1
(config-ike-client-pool)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

dns-server on page 5271
ip-range <start ip address> <end ip address> on page 5272
netbios-name-server <ip address> <secondary> on page 5273

dns-server

Use the **dns-server** command to specify the default primary and secondary domain naming system (DNS) servers to use for the Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the configured DNS server. Variations of this command include:

dns-server <*ip address*>
dns-server <*ip address*> <*secondary*>

Syntax Description

<*ip address*>	Specifies the IP address of the preferred DNS server on the network.
<*secondary*>	Optional. Specifies the IP address of the second preferred DNS server on the network. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, there are no specified default DNS servers.

Command History

Release 2.1	Command was introduced.
Release 4.1	Command was expanded to include the Internet key exchange (IKE) client configuration pool.

Usage Examples

The following example specifies a default DNS server with address **192.72.3.254** and a secondary DNS server with address **192.100.4.253**:

(config)**#crypto ike client configuration pool ConfigPool1**
(config-ike-client-pool)**#dns-server 192.72.3.254 192.100.4.253**

ip-range *<start ip address> <end ip address>*

Use the **ip-range** command to specify the range of addresses from which the router draws when assigning an IP address to a client. Use the **no** form of this command to remove defined IP ranges.

Syntax Description

<start ip address>	Specifies the first IP address in the range for this pool.
<end ip address>	Specifies the last IP address in the range for this pool. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

Default Values

By default, no IP address range is defined.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example defines an IP address range for this configuration pool:

(config)**#crypto ike client configuration pool ConfigPool1**
(config-ike-client-pool)**#ip-range 172.1.1.1 172.1.1.25**

netbios-name-server *<ip address> <secondary>*

Use the **netbios-name-server** command to specify the network basic input/output system (NetBIOS) Windows Internet Naming Service (WINS) name servers to assign to a client. Use the **no** form of this command to remove assigned name servers. Variations of this command include:

netbios-name-server *<ip address>*
netbios-name-server *<ip address> <secondary>*

Syntax Description

<ip address>	Specifies the primary WINS server IP address to assign.
<secondary>	Optional. Specifies the secondary WINS server IP address to assign.

Default Values

By default, no WINS server address is defined.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example defines two WINS server addresses for this configuration pool:

(config)**#crypto ike client configuration pool ConfigPool1**
(config-ike-client-pool)**#netbios-name-server 172.1.17.1 172.1.17.25**

IKE POLICY ATTRIBUTES COMMAND SET

To activate the Internet Key Exchange (IKE) Policy Attributes mode, enter the **attribute** command at the IKE Policy prompt. For example:

```
>enable
#configure terminal
(config)#crypto ike policy 1
(config-ike)#attribute 10
(config-ike-attribute)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

authentication on page 5275
encryption on page 5276
group on page 5277
hash on page 5278
lifetime <value> on page 5279

authentication

Use the **authentication** command to configure this Internet key exchange (IKE) policy's use of preshared secrets and signed certificates during IKE negotiation. Use the **no** form of this command to disable this feature. Variations of this command include:

authentication dss-sig
authentication pre-share
authentication rsa-sig

Syntax Description

dss-sig	Specifies to use DSS-signed certificates during IKE negotiation to validate the peer.
pre-share	Specifies the use of preshared secrets during IKE negotiation to validate the peer.
rsa-sig	Specifies to use RSA-signed certificates during IKE negotiation to validate the peer.

Default Values

By default, authentication is set to **pre-share**.

Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the signed certificates.

Functional Notes

Both sides must share the same preshared secret in order for the negotiation to be successful.

Usage Examples

The following example enables preshared secrets for this IKE policy:

(config-ike)**#attribute 10**
(config-ike-attribute)**#authentication pre-share**

encryption

Use the **encryption** command to specify which encryption algorithm this Internet key exchange (IKE) policy will use to transmit data over the IKE-generated security association (SA). Use the **no** form of this command to return to the default value. Variations of this command include:

encryption aes-128-cbc
encryption aes-192-cbc
encryption aes-256-cbc
encryption des
encryption 3des

Syntax Description

aes-128-cbc	Specifies the AES-128-CBC encryption algorithm.
aes-192-cbc	Specifies the AES-192-CBC encryption algorithm.
aes-256-cbc	Specifies the AES-256-CBC encryption algorithm.
des	Specifies the DES encryption algorithm.
3des	Specifies the 3DES encryption algorithm.

Default Values

By default, encryption is set to **DES**.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example selects **3DES** as the encryption algorithm for this IKE policy:

(config-ike)**#attribute 10**
(config-ike-attribute)**#encryption 3des**

group

Use the **group** command to specify the Diffie-Hellman Group (1, 2, or 5) to be used by this Internet key exchange (IKE) policy to generate the keys (which are then used to create the IPSec security association (SA)). Use the **no** form of this command to return to the default setting. Variations of this command include:

group 1
group 2
group 5

Syntax Description

1	Requires the IKE policy to use Diffie-Hellman Group 1 (768-bit modulus) exchange during IPSec SA key generation.
2	Requires the IKE policy to use Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPSec SA key generation.
5	Requires the IKE policy to use Diffie-Hellman Group 5 (1536-bit modulus) exchange during IPSec SA key generation.

Default Values

By default, group is set to **1**.

Command History

Release 4.1	Command was introduced.
Release 15.1	Command was expanded to include the **group 5** parameter.

Functional Notes

The local IKE policy and the peer IKE policy must have matching group settings in order for negotiation to be successful.

Usage Examples

The following example sets this IKE policy to use Diffie-Hellman Group **2**:

(config-ike)**#attribute 10**
(config-ike-attribute)**#group 2**

hash

Use the **hash** command to specify the hash algorithm to be used to authenticate the data transmitted over the Internet key exchange (IKE) security association (SA). Use the **no** form of this command to return to the default setting. Variations of this command include:

hash md5
hash sha

Syntax Description

md5	Choose the message digest 5 (MD5) hash algorithm.
sha	Choose the SHA hash algorithm.

Default Values

By default, hash is set to **sha**.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example specifies **md5** as the hash algorithm:

(config-ike)**#attribute 10**
(config-ike-attribute)**#hash md5**

lifetime <*value*>

Use the **lifetime** command to specify how long an Internet key exchange (IKE) security association (SA) is valid before expiring. Use the **no** form of this command to return to the default setting.

Syntax Description

<*value*>	Specify how many seconds an IKE SA will last before expiring. The valid range is **60** to **1209600**.

Default Values

By default, **lifetime** is set to **28800** seconds.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example sets a lifetime of two hours:

(config-ike)**#attribute 10**
(config-ike-attribute)**#lifetime 7200**

IKE POLICY COMMAND SET

To activate the Internet Key Exchange (IKE) Policy mode, enter the **crypto ike policy** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ike policy 1
(config-ike)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect on page 76
do on page 81
end on page 82
exit on page 83
interface on page 84

All other commands for this command set are described in this section in alphabetical order.

attribute <number> on page 5281
client authentication host on page 5282
client authentication host xauth-type on page 5283
client authentication server list <listname> on page 5284
client configuration pool <name> on page 5285
initiate on page 5286
local-id on page 5287
nat-traversal on page 5289
peer on page 5290
respond on page 5292

attribute *<number>*

Use the **attribute** command to define attributes for the associated Internet key exchange (IKE) policy. Multiple attributes can be created for a single IKE policy. Once you enter this command, you are in the IKE Policy Attribute mode. Refer to *IKE Policy Attributes Command Set on page 5274* for more information. Use the **no** form of this command to remove a defined attribute.

Syntax Description

<number>	Assigns a number (range: **1** to **65535**) to the attribute policy. The number is the attribute's priority number and specifies the order in which the resulting virtual private network (VPN) proposals get sent to the far end. This command takes you to the (config-ike-attribute)# prompt. From here, you can configure the settings for the attribute as outlined in the section *IKE Policy Attributes Command Set on page 5274*.

Default Values

By default, no **attribute** is defined.

Command History

Release 4.1	Command was introduced.

Functional Notes

Multiple attributes on an IKE policy are ordered by number (with the lowest number representing the highest priority).

Usage Examples

The following example defines a policy attribute (**10**) and takes you into the IKE policy attributes:

```
(config)#crypto ike policy 1
(config-ike)#attribute 10
(config-ike-attribute)#
```

client authentication host

Use the **client authentication host** command to enable the unit to act as an Xauth host when this Internet key exchange (IKE) policy is negotiated with a peer. Use the **no** form of this command to disable this feature. Variations of this command include the following:

client authentication host username <*username*>
client authentication host username <*username*> **password** <*password*>
client authentication host username <*username*> **password** <*password*> **passphrase** <*phrase*>

Syntax Description

password <*password*>	Specifies the value sent via Xauth as the password.
username <*username*>	Specifies the value sent via Xauth as the user name.
passphrase <*phrase*>	Optional. Specifies the value sent via Xauth as the passphrase. This is only used with authentication type one time password (OTP).

Default Values

By default, if this command is not present in the IKE policy, the unit does not act as an Xauth host.

Command History

Release 5.1	Command was introduced.

Functional Notes

The specified credentials are programmed into the unit, and there is no prompt for entering values real time. Therefore, schemes requiring real-time input or additional responses (e.g., SecureID) are not supported. The **client authentication host** and the **client authentication server** commands are mutually exclusive. Refer to *client authentication server list <listname> on page 5284* for more information.

Usage Examples

The following example specifies the login credentials to be sent:

(config)**#crypto ike policy 1**
(config-ike)**#client authentication host username jsmith password password1 passphrase phrase**

client authentication host xauth-type

Use the **client authentication host xauth-type** command to allow the user to specify the Xauth authentication type if a type other than **generic** is desired. Use the **no** form of this command to return to the default setting. Variations of this command include:

client authentication host xauth-type generic
client authentication host xauth-type otp
client authentication host xauth-type radius

Syntax Description

generic	Specifies generic authentication type.
otp	Specifies one time password (OTP) authentication type.
radius	Specifies remote authentication dial-in user service (RADIUS) authentication type.

Default Values

By default, authentication is set to **generic**.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command is used along with the **client authentication host username**. Refer to *client configuration pool <name> on page 5285* for more information. When acting as an Xauth host, this command allows the user to specify the Xauth authentication type if a type other than generic is desired.

Usage Examples

The following example sets the Xauth type to **radius**:

(config)**#crypto ike policy 1**
(config-ike)**#client authentication host xauth-type radius**

client authentication server list <*listname*>

Use the **client authentication server list** command to specify an authentication, authorization, and accounting (AAA) authentication method list to be used in the Internet key exchange (IKE) policy. AAA must be enabled to use this command (refer to the command *aaa on on page 1187*). Use the **no** form of this command to remove the authentication list from the policy. Variations of this command include:

client authentication server list default
client authentication server list <*listname*>

Syntax Description

default	Specifies the default AAA authentication method list is applied in the IKE policy.
<*listname*>	Specifies the named AAA authentication method list is applied in the IKE policy.

Default Values

By default, no AAA authentication method list is applied to the IKE policy and extended authentication is not performed.

Command History

Release 5.1	Command was introduced.

Functional Notes

When this IKE policy is negotiated and the peer has indicated Xauth via the IKE authentication method and/or the Xauth vendor ID, this command allows the unit to perform as an Xauth server (edge device). The specified AAA authentication method list is used to identify the location of the user authentication database.

The AAA authentication method list used by the IKE policy is most often the AAA login authentication method list. For more information about configuring these lists, refer to the command *aaa authentication login on page 1169*.

For more information about configuring AAA in your network, refer to the configuration guide *Configuring AAA in AOS* available online at https://supportcommunity.adtran.com.

Usage Examples

The following example specifies that the AAA authentication method list **AuthList1** is used in the IKE policy for extended authentication:

(config)**#crypto ike policy 1**
(config-ike)**#client authentication server list AuthList1**

client configuration pool <*name*>

Use the **client configuration pool** command to configure AOS to perform as mode-config server (edge device) when an Internet key exchange (IKE) policy is negotiated. Use the **no** form of this command to return to the default setting. Variations of this command include the following:

client configuration pool <*name*>
client configuration pool <*name*> **initiate**
client configuration pool <*name*> **initiate respond**
client configuration pool <*name*> **respond**
client configuration pool <*name*> **respond initiate**

Syntax Description

<*name*>	Specifies the pool from which to obtain parameters to assign to the client.
initiate	Enables set/ack (push) mode.
respond	Enables request/response mode.

Default Values

By default, if this command is not present in the IKE policy, the Adtran device allocates mode-config IP addresses, domain naming system (DNS) server addresses, and network basic input/output system (NetBIOS) name server addresses, and mode-config is not performed.

Command History

Release 4.1	Command was introduced.

Functional Notes

This command ties an existing client configuration pool to an IKE policy.

By using the **initiate** and **respond** commands, you can configure the IKE policy to initiate and respond, initiate only, or respond only. It is an error if you have both **initiate** and **respond** disabled.

Usage Examples

The following example ties the **ConfigPool1** configuration pool to this IKE policy:

(config)**#crypto ike policy 1**
(config-ike)**#client configuration pool ConfigPool1**

initiate

Use the **initiate** command to allow the Internet key exchange (IKE) policy to initiate negotiation (in main mode or aggressive mode) with peers. Use the **no** form of this command to allow the policy to respond only. Variations of this command include:

initiate aggressive
initiate main

Syntax Description

aggressive	Specifies to initiate using aggressive mode. Aggressive mode can be used when one end of the virtual private network (VPN) tunnel has a dynamically assigned address. The side with the dynamic address must be the initiator of the traffic and tunnel. The side with the static address must be the responder.
main	Specifies to initiate using main mode. Main mode requires that each end of the VPN tunnel has a static wide area network (WAN) IP address. Main mode is more secure than aggressive mode because more of the main mode negotiations are encrypted.

Default Values

By default, the **main** initiation mode is enabled.

Command History

Release 4.1	Command was introduced.

Functional Notes

By using the **initiate** and **respond** commands, you can configure the IKE policy to initiate and respond, initiate only, or respond only. It is an error if you have both **initiate** and **respond** disabled.

Usage Examples

The following example enables the AOS device to initiate IKE negotiation in main mode:

(config)**#crypto ike policy 1**
(config-ike)**#initiate main**

local-id

Use the **local-id** command to set the local ID for the Internet key exchange (IKE) policy. This setting overrides the system local ID setting (set in the Global Configuration mode using the **crypto ike local-id address** command). Use the **no** form of this command to remove a local ID. Variations of this command include:

local-id address <*ip address*>
local-id asn1-dn <*name*>
local-id fqdn <*name*>
local-id user-fqdn <*name*>

Syntax Description

address <*ip address*>	Specifies a remote IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
asn1-dn <*name*>	Specifies an abstract syntax notation distinguished name as the remote ID (enter this value in Lightweight Directory Access Protocol (LDAP) format).
fqdn <*name*>	Specifies a fully qualified domain name (FQDN) (e.g., **adtran.com**) as the remote ID.
user-fqdn <*name*>	Specifies a user FQDN or email address (e.g., **user1@adtran.com**) as the remote ID.

Default Values

By default, the local ID is not defined.

Command History

Release 4.1	Command was introduced.

Functional Notes

The local ID for a particular IKE policy can be set in two ways. The first (default) method is done in the Global Configuration mode:

(config)**#crypto ike local-id address**

This command, which by default is executed on startup, makes the local ID of an IKE policy equal to the IPv4 address of the interface on which an IKE negotiation is occurring. This is particularly useful for products that could have multiple public interfaces.

The second method is to use the IKE policy command:

(config)**#crypto ike policy 1**
(config-ike)**#local-id [address | asn1-dn | fqdn | user-fqdn]** <*ip address or name*>

This policy-specific command allows you to manually set the local ID for an IKE policy on a per-policy basis. You can use both methods simultaneously in the product. Several IKE policies can be created, some of which use the default system setting of the IPv4 address of the public interface. Others can be set to override this system setting and manually configure a local ID specific to those policies. When a new IKE policy is created, they default to **no local-id**. This allows the system local ID setting to be applied to the policy.

Usage Examples

The following example sets the local ID of this IKE policy to the IPv4 address **63.97.45.57**:

(config)**#crypto ike policy 1**
(config-ike)**#local-id address 63.97.45.57**

nat-traversal

Use the **nat-traversal** command to allow, force, or disable network address translation (NAT) traversal versions 1 and 2 on a specific Internet key exchange (IKE) policy. Use the **no** form of this command to disable this feature. Variations of this command include:

nat-traversal v1 allow
nat-traversal v1 disable
nat-traversal v1 force
nat-traversal v2 allow
nat-traversal v2 disable
nat-traversal v2 force

Syntax Description

v1	Specifies NAT traversal version 1.
v2	Specifies NAT traversal version 2.
allow	Sets the IKE policy to allow the specified NAT traversal version.
disable	Sets the IKE policy to disable the specified NAT traversal version.
force	Sets the IKE policy to force the specified NAT traversal version.

Default Values

The default values for this command are **nat-traversal v1 allow** and **nat-traversal v2 allow**.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example disables version **2** on IKE policy **1**:

(config)**#crypto ike policy 1**
(config-ike)**#nat-traversal v2 disable**

peer

Use the **peer** command to enter the IP address of the peer device. Repeat this command for multiple peers. Use the **any** keyword if you want to set up a policy that will initiate or respond to any peer. Use the **no** form of this command to remove a peer device. Variations of this command include:

peer <*ip address*>
peer any

Syntax Description

<*ip address*>	Specifies a peer IP address. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
any	Allows any peer to connect to this Internet key exchange (IKE) policy.

Default Values

No default values are necessary for this command.

Command History

Release 4.1	Command was introduced.

Functional Notes

An IKE policy is incomplete unless one of the peer commands is specified. Only one IKE policy can be configured with **peer any**.

Usage Examples

The following example sets multiple peers on an IKE policy for an initiate-and-respond policy using preshared secret, DES, message digest 5(MD5), and Diffie-Hellman Group 1:

(config)**#crypto ike policy 1**
(config-ike)**#peer 63.97.45.57**
(config-ike)**#peer 63.105.15.129**
(config-ike)**#peer 192.168.1.3**
(config-ike)**#respond anymode**
(config-ike)**#initiate main**

The following example sets up a policy allowing any peer to initiate using preshared secret, DES, MD5, and Diffie-Hellman Group 1.

(config)**#crypto ike policy 1**
(config-ike)**#peer any**
(config-ike)**#respond anymode**
(config-ike)**#initiate main**

Technology Review

IKE policies must have a peer address associated with them to allow certain peers to negotiate with the Adtran product. This is a problem when you have roaming users (those who obtain their IP address using Dynamic Host Configuration Protocol (DHCP) or some other dynamic means). To allow for roaming users, the IKE policy can be set up with **peer any** to allow any peer to negotiate with the Adtran product. There can only be one **peer any** policy in the running configuration.

respond

Use the **respond** command to allow the Internet key exchange (IKE) policy to respond to negotiations by a peer. Use the **no** form of this command to allow the policy to only initiate negotiations. Variations of this command include:

respond aggressive
respond anymode
respond main

Syntax Description

aggressive	Specifies to respond only to aggressive mode.
anymode	Specifies to respond to any mode.
main	Specifies to respond only to main mode.

Default Values

By default, respond to any mode is enabled.

Command History

Release 4.1	Command was introduced.

Functional Notes

By using the **initiate** and **respond** commands, you can configure the IKE policy to initiate and respond, initiate only, or respond only. It is an error if you have both **initiate** and **respond** disabled.

Usage Examples

The following example configures the router to initiate and respond to IKE negotiations:

(config)**#crypto ike policy 1**
(config-ike)**#respond anymode**

